Item 13
For Noting

Glasgow Kelvin College

Audit and Risk Committee – 17 May 2022

Risk Management Update

Report by Vice Principal Operations and Director of Corporate Services

1. Introduction

It is normal practice that the Strategic/College Risk Register is considered at every meeting of the Audit and Risk Committee, Risk Management Committee and is considered twice per year by the Board of Management, once per year by each of the other formal Sub Committees of the Board and reviewed by the College's Senior Management Team at least once a Quarter.

A copy of the Strategic/College Risk Register as at April 2022 is provided for information at **Appendix 1.**

2. Risk Management Activities

Since the last Audit and Risk Committee in February 2022 and Board Meeting in March 2022 a number of activities have taken place in relation to Risk Management:

- Risk Management Committee meeting held on 19 April 2022.
- Communication and Marketing Department Risk Register prepared – currently being finalised.
- Members of the SMT, Incident Management Team and Marketing Team attended the training on Crisis Communications & Public Relations after a Cyber Security Incident.
- The Learning and Teaching Committee have undertaken their annual review of the Strategic/College Risk Register.

3. Risk Register Review

The Risk Title, Residual Risk Score and colour of the thirteen risks which could impact on the College's ability to deliver its strategic ambitions are summarised in the table below including Inherent Risks Scores/Categories and Residual Risks Scores/Categories.

Risk Nº	Date Identified	Risk Title	IR	IR2	RR	RR2	Risk Appetite Category	Movement in Period
1	Nov 21	SFC Review	20	Very High	12	High	1. Policy	↔
2	Nov 21	GKC Identity	16	Very High	9	High	2. Reputation	↔
3	Nov 21	People	20	Very High	9	High	5. Workforce	↑
4	Nov 21	Litigation / Compliance	16	Very High	6	Medium	7. Legal & Compliance (inc. H&S risks)	↑
5	Nov 21	Curriculum Relevance	16	Very High	9	High	6. Student Experience	↔
6	Nov 21	Sustainable Funding	16	Very High	12	High	3. Financial	↔
7	Nov 21	Student Experience	16	Very High	9	High	6. Student Experience	↔
8	Nov 21	Environment	16	Very High	9	High	8. Environmental Sustainability	↔
9	Nov 21	Digital Transformation	16	Very High	6	Medium	4. Digital	↔
10	Nov 21	Student Recruitment & Retention	20	Very High	12	High	6. Student Experience	↔
11	Nov 21	Cyber Risk	25	Very High	12	High	2. Reputation	↔
12	Dec 21	COVID-19 - Ongoing Implications	16	Very High	9	High	1. Policy	↓
13	Apr 22	Strike Action	25	Very High	16	Very High	6. Student Experience	New

The College considers risks on an ongoing basis, these include:

- Covid-19 and related negative effects on credits/delivery/students/staffing/ resources.
- An emerging/changed world/hybrid learning and teaching/working/the job market.
- Brexit and related negative effects on staffing, contractors and supplies i.e. shortages with suppliers now unable to meet deadlines.
- The impacts of the Climate Emergency.
- The Review of Coherent Provision and Sustainability of the Glasgow Region.
- Inflation/cost of living, high energy and ever-increasing food prices and the very negative impact on standards of living for everyone but particularly the lowest income households will feel this the most.
- National Insurance increases (April 2022).
- Increase in Living Wage costs.
- Mental health decline with some individuals fearful of going outside; COVID-19 impact.
- National Health Service has unprecedented delays to operations; the health of the nation will decline and the impact will be felt by the College.
- Cybersecurity threats are growing – from 2020, malware and ransomware attacks increased by 358% and 435% respectively outpacing the ability to respond to them effectively. In relation to our impending cyber security renewal, we are advised that the cyber insurance market has hardened considerably over the last 12-18 months, premiums have increased dramatically and underwriting requirements are far stricter than they have even been before.
- NJNC – Strike Action on the following dates:
  - Wednesday 20 April 2022
  - Tuesday 26 and Wednesday 27 April 2022
  - Wednesday 4 and Thursday 5 May 2022
  - Thursday 12 May 2022
  - Tuesday 17, Wednesday 18, and Thursday 19 May 2022 (TBC, two of these dates may be cancelled but no formal notification has been received at the time of writing this report)

- Tuesday 24, Wednesday 25, and Thursday 26 May 2022 (TBC, two of these dates may be cancelled but no formal notification has been received at the time of writing this report)

- Action short of strike action (ASOS) and withdrawal of goodwill by EIS members also advised.
- At the time of writing this report, UNISON are currently balloting for strike action – outcome awaited.
- Budget Cuts for 2022-25.
- SFC – In Year Redistribution of Credit Activity for AY 2021-22.
- Foundation Apprenticeship delivery/Voluntary Severance Scheme being offered to team members due to changes to regional delivery.
- Ukraine/Russia conflict is resulting in warnings of increased likelihood of cyber-attacks i.e. on national infrastructure, defence companies, oil and gas infrastructure providers, financial instructions and government.
- Energy prices are forecasted to massively increase; gas on average by 232% and electricity by 41% as indicated by APUC/Procurement Scotland; this equates to an additional estimated total price of over £400k per annum for the College.
- The energy price hikes will place severe financial pressures on the already disadvantaged communities the College serves with many households unable to afford food and heating resulting in untold misery that will get worse as we head into autumn and winter.
- The College insurance company have advised of an almost weekly incident of student suicide.
- The wellbeing of any Russian employees needs to be fully considered.

4. Fire Risk Assessment

As reported at the previous Audit and Risk meeting, an annual fire risk assessment was carried out at all campuses; the final reports are available for review via the following link:

Link to Fire Risk Assessment reports

All actions referred to in these reports have been extracted and are contained within an Action Plan which is being worked through; this is attached as at **Appendix 2.**

5. Cladding

As reported at the last Audit and Risk meeting, during a period of extremely windy weather, a very small cladding panel was dislodged from the Springburn Campus building. Checks of all panels were carried out and a report was provided in relation to the findings. The report can be reviewed via the following link:

Link to the Springburn Campus Cladding Report

During the period between the checks being conducted and the report being generated, a large panel (at ground level) became dislodged and was discovered on the ground in pieces. There is no reason known as to why this happened. This panel was not on the report as referred to in the above paragraph and Struan have taken the broken panel to ascertain why this fell. Advice currently awaited.

Liaison has taken place with the College insurance company in relation to this matter and to provide them with the report received from Struan. The report from Struan identified a number of cracked panels and also a large number panels which are displaying rust spots; the cause of these cracks and rust spots is not 100% clear.

A structural survey has been ordered by another company we have used previously to ascertain what is causing the rust spots and why some panels are cracking. For this survey to be conducted we need an appropriate panel removed by a specialist company. The areas under where the cracked panels are located have been cordoned off (as per our insurance company request) in case they fall; although this is considered to be unlikely. Members should note that replacement panels have been ordered via the only company that supplies these – based in France. Replacement panels are taking several months to arrive due to Brexit and Covid-19 related issues.

When the cause of the rust spots and cracking tiles is known via this structural survey; the College will take any necessary steps required to rectify the situation.

Audit and Risk members will be kept apprised of this situation; this matter has been added to the Corporate Risk Register.

6. Chemical Leak at Springburn Campus

On 11 March 2022, there was a chemical leakage in our Springburn Campus. The building was promptly evacuated and the emergency services dealt with the situation. A full report was generated and discussed at SMT – refer to **Appendix 3**. All actions contained in this report are being undertaken at present (refer to the Strategic/ College Risk Register.)

7. Vandalism at East End Campus

After one month of added security, the vandalism at East End Campus Community Garden appears to have ceased.

8. Insurance Conference

L Clark attended the annual conference on 30 March 2022; emerging trends in relation to claims are:

- Discrimination
- Sexual Misconduct
- Data Breach Claims
- Employment Tribunal Claims
- Personal Injury Damages
- Claimant Legal Costs
- Unrepresented Claimants
- Escape of Water

The above matters have been discussed with the Risk Management Committee members.

9. Student Experience/Performance Indicator Data

A recent Scottish Government report stated that the number of college students in Scotland leaving their studies saw an increase during the pandemic.

The report also warned that drop-out rates could rise further and this year's college enrolment was "considerably down".

The report, which focused on the "indirect, wider harms of the pandemic", said that although the 2021-22 session has been closer to what it was pre-Covid there was still "an on-going cumulative wider impact on students and learners".

It looked at three areas including:

- higher education;
- further education;
- and community learning and development in Scotland.

The report said that some of the wider harms "would not be unique to these sectors and are also likely to have affected other groups".

In its focus on colleges the paper said: "College and student representatives explained that the number of students dropping out of courses has increased. Further increases in drop-out rates remains a serious risk and new entrants who started in January 2022 are another at-risk cohort."

It went on to explain that the overall numbers of college enrolments were "considerably down in the current academic year" due to a number of factors.
More pupils had opted to stay on at school and more school pupils had secured university places. Added to that, there had been a greater availability of low skilled jobs and college course numbers had been capped as a result of physical distancing requirements.

The latest leaver destination survey, published in February 2022, indicated that the proportion of school leavers at either university or college had increased from 44.2% in 2019-20 to 45.1% in 2020-21.

The proportion of school leavers in further education fell from 28.1% to 23.3% and the proportion of school leavers who were unemployed fell from 6.0% to 4.2%.

10. Budget Cuts for 2022-25

The Draft Budgets for 2022-25 were presented to the Finance & Resources Committee for endorsement on 10 May 2022 and will go to the Board on 13 June 2022 for approval.

While the financial measures built into the budgets will allow the College to remain stable over the next three years, they represent significant challenges and may impact on student experience and staff morale. The approach adopted is not sustainable basis for long term financial planning or effective running the College.

11. SFC – In Year Redistribution of Credit Activity for AY 2021-22

The Quarter 2 Financial Forecast reflects the potential clawback of funding for 2,100 credits, estimated at c£480k. SFC/GCRB have not confirmed that this clawback will actually take place and it is unlikely that this will be confirmed until at least the end of the financial year. In addition, there is a risk that any additional under delivery of credits may also be subject to clawback and this will be taken into account for the Quarter 3 Forecast. The position continues to be closely monitored, but the uncertainty makes accurate financial forecasting very difficult.

12. Land at Springburn

The Vice Principal – Operations, Director of Corporate Services and Head of Facilities and Environmental Sustainability met with members of Hydepark Residents Association to discuss the amenity land where the Cycle Hub is situated. The College has received a valuation for this parcel of land.

A further meeting has been held with the Director of Corporate Services, Head of Facilities and Environmental Sustainability and the Factor for the Hydepark Residents Association. The Factor has advised that he is obtaining his own valuation for this piece of land. At the time of writing this report, this valuation is awaited.

Audit and Risk members will be kept apprised of this situation.

13. Risk Management Committee

At the recent Risk Management Committee meeting held on 19 April 2022, due cognisance was taken of key risk reports/publications/newsletters; links provided below:

Audit Scotland: Fraud and Irregularity
BCI Horizon Scan Report
WEF: The Global Risks Report 2022
HEFESTIS Newsletters from 15 December 2021 to 4 April 2022

The approved minute of the Risk Management Committee held on 25 January 2022 is provided for interest and perusal; link below:

Risk Management Minute – 25 January

14. Glasgow Kelvin College and Rostov on Don

Members will be aware that the College has a current Memorandum of Understanding with the Don State Technical University in Rostov on Don, Russia. This is a very fruitful and long-standing student/staff exchange programme ran in conjunction with University of the West of Scotland and involving the Lord Provost and International Department at Glasgow City Council. However, this has been suspended via Glasgow City Council as per the link below:

https://www.glasgowlive.co.uk/news/glasgow-suspends-russian-town-twinning-23205531

15. Resource Implications

There are additional resource implications in relation to items referred to in this report i.e. cover for staff members on sickness leave due to COVID or COVID related issues, additional support needed for staff/students in relation to eg mental health matters. The cladding inspection outcome may also yield unexpected costs.

16. Risk & Assurance

There are no risks or perceived implications arising from this report that are not already recorded in the Risk Register or this paper. The strike action, action short of strike action (ASOS), the withdrawal of goodwill from EIS teaching members coupled with the threat of strike action from UNISON employees, places considerable strain on College operations and severely and very negatively disrupts the student experience which has not been a positive one for some time due to Scottish Government COVID-19 lockdowns and "on campus" restrictions. Failure to educate claims are therefore a very real possibility.

17. Equality

There are no adverse impacts on individuals with protected characteristics arising from the contents of this report. As contained within this report, poverty is prevalent throughout the communities the College serves and there is a greater risk of student drop-out rates or non-engagement due to a wide number of factors such as rising living costs, many emerging mental health issues and a declining standard of living due to a wide number of factors.

18. Data Protection

There are no new data protection risks arising from the contents of this report. Data protection continues to be a key consideration in College activities.

19. Recommendations

Members of the Audit and Risk Committee are recommended to note the contents of this report, links and appendices.

20. Further Information

Members can obtain further information on the contents of this report from Jeanette Evans, Vice Principal Operations at jevans@glasgowkelvin.ac.uk or Lisa Clark, Director of Corporate Services at lisaclark@glasgowkelvin.ac.uk

JE/LC
Glasgow Kelvin College – May 2022

GLASGOW KELVIN COLLEGE - College/Strategic Risk Register

Appendix 1

Board / Committee	
Prepared by: Jeanette Evans/Lisa Clark	
Contact Name and Tel. No.:	

						INHERENT ASSESSMENT					RESIDUAL ASSESSMENT										
Risk Ref No	Date Identified	Risk Title	Risk Description	Risk Owner	Responsible Person	IL	II	IR	IR	Controls and Mitigating Actions	RL	RI	RR	RR	Risk Appetite Category	Risk Appetite	Risk Treatment Approach	Date Reviewed	Movement in Period	Early Warning Mechanisms, Planned Next Steps & Future Action Required	Date of Next Review
1	04/11/2021	SFC Review	**RISK:** Being forced into position that is against our vision & mission, or reduces community engagement, e.g. A single governing body for Glasgow **CAUSE:** Failure to project a clear GKC identity or vision; failure to proactively engage in review; other voices are louder / stronger; or poor operating performance. **EFFECT:** Lose local autonomy; unable to meet local community needs; GKC identity is lost; loss of social footprint; loss of staff.	Principal & CEO / Chair	Vice Principal - Curriculum	4	5	20	**Very High**	1. Engagement with GCRB, SFC, Scot Gov, & UK Gov 2. Political engagement with local & national politicians 3. Engagement about possible models with other colleges 4. Board understanding & support 5. Identified forums where we can share our vision 6. Direct community engagement 7. Improved operating position & management of performance 8. Identifed awards & other opportunities to raise profile 9. Interaction with Scot Gov officials 10. Operational collaboration projects with other colleges	3	4	12	**High**	1. Policy	Cautious	Treat	19/04/2022	↔	**Early Warning Mechanism** 1. Outcome of consultants options appraisal 2. Ministerial responses / statements from Scot Gov 3. Performance Monitoring 4. GCRB Comms **Actions Planned** 1. Develop a college strategy for stakeholder consultation 2. Improving recruitment & student outcome performance 3. Continuing to influence GCRB decision making 4. Identify opportunities to collaborate	16/08/2022
2	04/11/2021	GKC Identity	**RISK:** Lack of understanding or awareness of the critical part GKC plays in communities; don't communicate USP **CAUSE:** Do not proactively promote identity, successes & uniqueness of GKC; ineffective comms on identity & successes; failure to illustrate impact we have; underinvestment in marketing / messaging. **EFFECT:** Weak employer engagement; students choose another college; affects risk no. 1	Vice Principal - Operations		4	4	16	**Very High**	1. Tendering for new website 2. Developing new internal & external comms & marketing framework (in train) 3. Actively seeking to promote successes 4. Faculties using own social media 5. Investment in marketing resource 6. Employer engagement activity 7. Awards - putting forward GKC 8. Community Engagement, e.g. Hub 9. Digital strategy / My Kelvin	3	3	9	**High**	2. Reputation	Minimalist	Treat	19/04/2022	↔	**Early Warning Mechanism** 1. Negative publicity 2. Poor recruitment figures **Actions Planned** 1. Review of Comms & Marketing resource 2. Strategic Priority to raise profile 3. Campus Project 4. New website 5. Comms & Marketing Framework being developed	16/08/2022
3	04/11/2021	People	RISK: Not having agile, motivated, well-informed, or appropriately skilled workforce CAUSE: Demographics of workforce; national bargaining; Notiication of strike dates by EIS and notification of a ballot for strike action from UNISON - impact of strike action on employment relations; lack of / insufficient CPD; failure to attract talented individuals; failure to retain talented individuals; unable to predict needs of the future; affordability of job evaluation. EFFECT: Unable to compete with industry; staff ability to be innovative is restricted; unable to deliver curriculum in areas of student demand; morale; financial stability.	Dir. Human Resources		5	4	20	**Very High**	1. People Strategy 2. Representation in employers association 3. NJNC negotiator 4. OD framework 5. TU engagement 6. RPA 7. TRCC 8. Recruitment & Retention Policies & Procedures 9. Culture of empowerment 10. 3 Year Rolling Budgets	3	3	9	**High**	5. Workforce	Cautious	Treat	19/04/2022	↑	**Early Warning Mechanism** 1. Staff turnover 2. Absences 3. HR Heatmap **Actions Planned** 1. Workforce Planning 2. Continuous improvement programme	16/08/2022

Appendix 1

GLASGOW KELVIN COLLEGE - College/Strategic Risk Register

Board / Committee	
Prepared by: Jeanette Evans/Lisa Clark	
Contact Name and Tel. No.:	

						INHERENT ASSESSMENT					RESIDUAL ASSESSMENT										
Risk Ref No	**Date Identified**	**Risk Title**	Risk Description	**Risk Owner**	**Responsible Person**	**IL**	**II**	**IR**	**IR**	**Controls and Mitigating Actions**	**RL**	**RI**	**RR**	**RR**	**Risk Appetite Category**	**Risk Appetite**	**Risk Treatment Approach**	**Date Reviewed**	**Movement in Period**	**Early Warning Mechanisms, Planned Next Steps & Future Action Required**	**Date of Next Review**
4	04/11/2021	Litigation / Compliance	**RISK:** Non-compliance with key legislative or regulatory requirements including COSHH **CAUSE:** Lack of awareness, understanding or training & development; poor compliance with established processes; not keeping up to date with changes in case law. **EFFECT:** Possible fines & litigation; reputational damage; implications for board accountability.	Dir of Corporate Services / & Dir Human Resources / H&S Manager		4	4	16	**Very High**	1. Policies & procedures 2. Members of national groups to keep aware of developments & upcoming changes. 3. Horizon scanning for changes to legislation or regulations. 4. Legal advice. 5. CPD programme. 6. Staff training. 7. Internal & external audit programme provides assurance. 8. External DPO. 9. Liaison as required with College insurance.	2	3	6	**Medium**	7. Legal & Compliance (including Health & Safety risks)	Averse	Treat	19/04/2022	↑	**Early Warning Mechanism** 1. Horizon scanning 2. HR Heatmap 3. Compliance metrics **Actions Planned** 1. RIDDOR Report to HSE. 2. COSHH Custodians appointed. 3. COSHH Audit undertaken over 2 days. 4. All departments and faculties directed to conduct reviews of their COSHH inventories/storage. 5. Deadline for legally mandated training brought forward. 6. WorkRite COSHH module made available to additional staff. 7. Six respirators ordered to enhance any future emergency response.	16/08/2022
5	04/11/2021	Curriculum Relevance	RISK: Curriculum doesn't meet current or future needs of students, employers, or community partners, or the economy CAUSE: Ageing workforce; lack of curriculum innovation; staff knowledge & expertise; People risk (Risk No. 3); employer engagement; outdated or lack of resources; unreliable information / data; growth of digital teaching / you tube. EFFECT: Diminishing recruitment; reputation; student achievement; reputation.	Vice Principal - Curriculum		4	4	16	**Very High**	1. Curriculum reviews 2. Staff training / CPD 3. Emp engagement 4. Schools engagement 5. Partners - HE 6. Labour market intelligence 7. Staff structures / PDR 8. Industry bodies 9. Student feedback 10. Collaboration with partners & colleges 11. Digital transformation	3	3	9	**High**	6. Student Experience	Open	Treat	19/04/2022	↔	**Early Warning Mechanism** 1. Recruitment & retention of students 2. Emp & student feedback 3. Success rates 4. HN Next Generation Monitoring **Actions Planned** 1. Strengthen CPD for staff 2. Strengthen Curriculum review 3. Digital / blended development 4. Targeted employer engagement 5. Creation of Centres of Excellence 6. Green Kelvin	16/08/2022
6	04/11/2021	Sustainable Funding	RISK: Inability to secure appropriate levels of funding to deliver objectives/Foundation Apprenticeship arrangements changing, re-distribution of credit activity for 2021-22, NI costs rising, inflation high, energy prices soaring. CAUSE: constraints of current funding structures & levels; budget cuts; Scot Gov / SFC funding models; constraints in public finances; non-compliance EFFECT: loss of income; inability to deliver financially sustainable budgets; med-long term sustainability at risk; impact on curriculum delivery; job losses	Vice Principal - Operations		4	4	16	**Very High**	1. 3 year budgets 2. Management accounting & budgetary control 3. Quarterly budgets & forecasting 4. TRCC 5. Compliance framework - review, monitor & control of funding obligations 6. Annual internal audit programme 7. Funding officer in Business Development team 8. Underlying cash position to agreed levels.	4	3	12	**High**	3. Financial	Cautious	Treat	19/04/2022	↔	**Early Warning Mechanism** 1. Negative variances 2. Quarterly reviews 3. Budget reviews 4. Nov SFC Nov cut-off 5. Credit delivery levels. **Actions Planned** 1. Enhancing business intelligence on funding streams 2. Building ALF 3. Curriculum planning 4. Identify alternative funding streams/Business Development Ambitions	16/08/2022

GLASGOW KELVIN COLLEGE - College/Strategic Risk Register

Appendix 1

Board / Committee	
Prepared by: Jeanette Evans/Lisa Clark	
Contact Name and Tel. No.:	

						INHERENT ASSESSMENT					RESIDUAL ASSESSMENT										
Risk Ref No	Date Identified	Risk Title	Risk Description	Risk Owner	Responsible Person	IL	II	IR	IR	Controls and Mitigating Actions	RL	RI	RR	RR	Risk Appetite Category	Risk Appetite	Risk Treatment Approach	Date Reviewed	Movement in Period	Early Warning Mechanisms, Planned Next Steps & Future Action Required	Date of Next Review
7	04/11/2021	Student Experience	**RISK:** Poor student experience **CAUSE:** Poor physical environment; quality of teaching; lack of teaching skills or resources; lack of support services, impact of industrial action and impact of COVID/long COVID on absence rates. **EFFECT:** Impact on retention of students; reputational damage among possible future students; financial instability; performance outcomes affected; relationship with employers; failure to deliver Government ambitions	Vice Principal - Curriculum		4	4	16	Very High	1. Curriculum quality assurance 2. Quality framework 3. Curriculum Planning 4. Student feedback 5. Engagement with Student association 6. Learning & support services/in campus services 7. CPD for staff 8. Investment in estate 9. Planned & routine maintenance 10. Operational planning process has Student Engagement at heart 11. GTCS Strategy	3	3	9	High	6. Student Experience	Open	Treat	19/04/2022	↔	**Early Warning Mechanism** 1. Student numbers metrics 2. Student destination **Actions Planned** 1. Campus Project 2. Retention improvement plan 3. Quality system review & development 4. Business Intelligence reporting & monitoring 5. Learner engagement 6. GTCS Strategy 7. Student Association Questionnaires/Feedback and addressing any complaints	16/08/2022
8	04/11/2021	Environment	**RISK:** College fails to meet targets in relation to sustainability, e.g. Net Zero **CAUSE**: Lack of resources to implement; lack of skills to implement; sustainability is not embedded within curriculum; cannot access funding; limited by pace of industry **EFFECT**: Do not meet targets; impact on future generations; reputation with students, future students, community & government affected	Vice Principal - Operations / Director of Corporate Services		4	4	16	Very High	1. Public Sector Climate Change Report completed annually. 2. Funding to recruit Environmental Manager secured from the SCIO for 2 years. 3. Individual appointed and start date awaited. 4. Environmental Manager will raise environmental awareness & access funding streams. 5. Green Kelvin initative is a key strategic priority. 6. Awareness raising activity paramount.	3	3	9	High	8. Environmental Sustainability	Minimalist	Treat	19/04/2022	↔	**Early Warning Mechanism** 1. PSCC metrics **Actions Planned** 1. Recruitment of Environmental Manager - start date awaited 2. Implementation of Green Kelvin action plan 3. CPD 4. Curriculum changes	16/08/2022
9	04/11/2021	Digital Transformation	**RISK:** Inability to deliver Digital Transformation Strategy & Programme **CAUSE:** Lack of resources to implement; lack of skills to implement; user skills insufficient; poor change or project management **EFFECT:** Reputation with students & staff affected; operational effectiveness reduced; student experience deteriorates	Vice Principal - Curriculum / Director of Digital Services		4	4	16	Very High	1. Strategy & Programme 2. Staffing structure to support delivery 3. Increased resources to implement 4. Staff training & awareness 5. New software 6. Website tendering 7. Increased devices available to staff & students 8. Programme management / governance	2	3	6	Medium	4. Digital	Cautious	Treat	19/04/2022	↔	**Early Warning Mechanism** 1. Missed deadlines / milestones **Actions Planned** 1. Implementation of programme: further development of business intelligence for learning & teaching development 2. Continuation of staff training	16/08/2022
10	04/11/2021	Student Recruitment & Retention	**RISK:** Fail to Recruit or Retain Sufficient students or learners **CAUSE:** Effectiveness of admissions process; monitoring of information; lack of identity; ineffective marketing; curriculum offer does not meet student needs **EFFECT:** Students do not get access to quality learning & teaching; class sizes are not sustainable; reduced funding; additional expenditure; COVID-19 mental health challenges; impact on PI's/sucess rates.	Vice Principal - Curriculum		5	4	20	Very High	1. Admissions process 2. Marketing 3. Monitoring attendance & performance 4. Wellbeing Lead appointed to engage with student body. 5. Wellbeing Officers appointed. 6. Keep warm events. 7. Student Support Services Manager appointed.	3	4	12	High	6. Student Experience	Cautious	Treat	19/04/2022	↔	**Early Warning Mechanism** 1. Student recruitment metrics 2. Drop out metrics **Actions Planned** 1. Campus Re-investment Project running to improve student experience. 2. Student focussed teams.	16/08/2022
11	04/11/2021	Cyber Risk	**RISK:** A widespread cyber-attack breaches college defence **CAUSE:** A malicious breach of college systems possibly caused by: user error / lack of training or education; lack of patch management; failure of perimeter security; poor development practices; lack of investment in protection **EFFECT:** Loss of business critical systems; college reputation damaged / loss of credibility; impact on individual people (data subjects); possible fines or litigation; cost to repair or restore; impact on students / student experience	Vice Principal - Curriculum / Director of Digital Services		5	5	25	Very High	1. Automated patch management 2. Mandatory training for all college employees 3. Firewall & DNS protection 4. MFA (multi-factor authentication) controls 5. Safelinks 6. Information security policy 7. Anti-virus & malware scans 8. Development frameworks 9. Knowledge sharing with peers 10. Cyber security insurance 11. Disaster Recovery / Business Continuity Plan in place - including backups 12. Crisis comms training attended on cyber attacks.	3	4	12	High	2. Reputation	Minimalist	Treat	19/04/2022	↔	**Early Warning Mechanism** 1. Monitoring of key systems performance & availability 2. Log management / monitoring 3. Monitoring of open source cyber intelligence, websites etc. **Actions Planned** 1. Review need for zero-trust architecture 2. Review how embedded mandatory training is for all staff	16/08/2022

Appendix 1

GLASGOW KELVIN COLLEGE - College/Strategic Risk Register

Board / Committee	
Prepared by: Jeanette Evans/Lisa Clark	
Contact Name and Tel. No.:	

						INHERENT ASSESSMENT					**RESIDUAL ASSESSMENT**										
Risk Ref No	**Date Identified**	**Risk Title**	Risk Description	**Risk Owner**	**Responsible Person**	**IL**	**II**	**IR**	**IR**	**Controls and Mitigating Actions**	**RL**	**RI**	**RR**	**RR**	**Risk Appetite Category**	**Risk Appetite**	**Risk Treatment Approach**	**Date Reviewed**	**Movement in Period**	**Early Warning Mechanisms, Planned Next Steps & Future Action Required**	**Date of Next Review**
12	13/12/2022	COVID-19 - Ongoing Implications	**RISK:** Ongoing negative impact of COVID-19 on all aspects of College operations. **CAUSE:** COVID/Long COVID ~~New virus strains~~ causing higher/ongoing levels of staffing absence due to illness/self-isolation. Staff members at work feeling under increased pressure. Individuals living in a constant state of fear for circa 2 years has resulted in mental health deterioration/issues related to anxiety/lack of confidence. Return to study/work/hybrid model causing feelings of unease. PCR testing/social distancing ending which may cause further unease. **EFFECT:** Loss of business, reduced student learning experience, higher than normal drop out rates/absence; high costs for staff cover, college reputation damaged/loss of credibility; very negative impact on different groups of people.	Principal & CEO / Chair		4	4	16	**Very High**	1. Discussions taking place about a hybrid model of working to enable people to start to think about this. 2. Enhanced cleaning regime remains in place throughout the campus buildings. 3. Social distancing ending ~~in place.~~ 4. Rooms ventilated if at all possible; upgrade to ventilation system at Springburn Campus. 5. Relatively low numbers of people in campus buildings/hybrid working will ensure this is still low, however, there are no campus restrictions. 6. Scottish Government COVID aware signage in place. 7. Anti-virus hand sanitiser and wipes available across the entire campus. 8. Masks available. 9. ~~External signage.~~ 10. ~~LFD tests available.~~ 11. Wellbeing high on the agenda for the College student and staff population.	3	3	9	**High**	1. Policy	Cautious	Treat	19/04/2022	↓	**Early Warning Mechanism** 1. Monitoring of Scottish Government messages 2. Management/monitoring of staffing situations 3. Monitoring of positive test cases/health issues **Actions Planned** 1. Keeping abreast of Scottish Government's guidance 2. Keep a close watch on staffing levels and cover required 3. Enhanced cleaning regime to remain in place	16/08/2022
13	19/04/2022 NEW RISK	Strike Action	**RISK:** Negative impact of teaching strike action on students coupled with the threat of action short of strike action (marking of assessments) with an additional threart of support staff strike action to follow. **CAUSE:** Teaching staff are requesting a better pay offer than they have received. This is a national matter and is being handled at a national level. At present there are 14 days of teaching strike action underway. **EFFECT:** Very negative impact on students who are only beginning to return to on-campus teaching. Lack of confidence in Colleges to provide the FE Training they require as strike action is an ever present threat and has been for many years. Drop out rates increase which has a negative effect on funding and PI's. Opportunity for HE institutions to deliver course requirements. Strike action could have a very detrimentall effect on the sector as a whole. Students may submit a "failure to educate" claim.	SMT (national matter)	This is a national matter.	5	5	25	**Very High**	1. Principal and Director of HR involved in national talks. 2. Meetings taking place at national level to attempt to resolve the situation. 3. Monitoring of impact on teaching delivery and identification of potential mitigations for lost learning. 4. College support staff offering whatever help they can to students.	4	4	16	**Very High**	6. Student Experience	Open	Treat	19-Apr-22		**Early Warning Mechanism** 1. Monitoring of Scottish Government/national Employer Association messages. 2. Senior management attending Employer Association meetings as required. 3. Principal and Director of HR involved in national discussions. 4. Monitoring staff particiaption levels in strike activity. **Actions Planned** 1. Keeping abreast of all related documentation/discussions. 2. Keep a close watch on effect on student population and identify potential mitigations to recover lost learning.	16/08/2022

Glasgow Kelvin College - Fire Risk Assessment February 2022 – Action Plan by Campus

Campus:	East End							
Category 5: Means of Escape								
Question	**Non-Conformity**	**Recommendations**	**Risk Level**	**Location**	**Required Completion Date**	**Person/s Responsible**	**Progress/Comments**	**Date Completed**
Do the fire resisting door sets meet the appropriate standard?	On 1st floor level there is an office suite with entry from both atrium and escape corridor therefore crossing over two compartments.	The door in the corridor does not have a self-closing device fitted. As this door is not required it is recommended that it be kept locked shut to maintain means of escape.	Medium		18/03/2022	G Lawson	Door locked and signage added to both sides	07/03/2022
Do the fire resisting door sets meet the appropriate standard?	The fire doors have a large gap between the doors and the frame which may prevent the intumescent seals being effective.	The doors should be adjusted to ensure that there is no more than a 3mm gap between the hinge edge, leading edge, and the top of the door frame.	Medium		18/03/2022	Joiner Technician	**Ongoing**	
Category 10: Management								
Question	**Non-Conformity**	**Recommendations**	**Risk Level**	**Location**	**Required Completion Date**	**Person/s Responsible**	**Progress/Comments**	**Date Completed**
Have employees received appropriate fire safety awareness training?	Fire marshals/wardens training overdue.	Employees expected to fulfil a role of a fire marshal/warden will require comprehensive training from a competent person/organisation to cover all of their additional responsibilities. It should be remembered that for each fire marshal/warden required a deputy should be trained to cover any absences. In addition, a fire marshal/warden should take no longer than one minute to search a designated area.	Medium		18/03/2022	G Lawson	**Training underway – New East End Fire Wardens trained**	
Category 11: Signs and Signals								
Question	**Non-Conformity**	**Recommendations**	**Risk Level**	**Location**	**Required Completion Date**	**Person/s Responsible**	**Progress/Comments**	**Date Completed**
Are there adequate and suitable fire safety signs and notices displayed in the appropriate places throughout the premises?	Fire action notices have not Been provided.	Fire action notices must be installed in all the common areas within the building and adjacent to the fire alarm call points. They are to contain the relevant information to aid a safe escape from the building.	Low		17/05/2022	G Lawson	All signs replaced or updated	07 March 2022
Are there adequate and suitable fire safety signs and notices displayed in the appropriate places throughout the premises?	A number of fire action notices were found to be defaced or incomplete.	The notices should be completed in full with the location of the assembly point and the number to call in an emergency.	Low		17/05/2022	G Lawson	All signs replaced or updated	07 March 2022

Campus:	Easterhouse							
Category 2: Sources of Ignition								
Question	**Non Conformity**	**Recommendations**	**Risk Level**	**Location**	**Required Completion Date**	**Person/s Responsible**	**Progress/Comments**	**Date Completed**
Are all electrical installations and appliances correctly installed and maintained?	There is unsafe use of extension leads. Daisy chaining	These appliances are to be used in accordance with manufacturers' instructions or alternatively, additional power sockets provided in this area.	Medium	T04	18/03/2022	ICT	Extensions piggybacked to each other instead of buying in the appropriate length of cabling. Extension removed. The photo provided did not match the room indicated on the site map. Recommend all staff are reminded not to set up any extensions this way.	22/03/22
Are all electrical installations and appliances correctly installed and maintained?	There was no evidence of periodic inspections of the lift installations.	If evidence of an inspection is unavailable, a competent person is to inspect the lift installations and records maintained.	Low	Lift	17/05/2022	Kone	The lifts are maintained monthly by Kone and annually by Ashdale for our insurance company. Paperwork uploaded to the electronic logbook.	22/03/22
Category 3: Sources of Fuel								
Question	**Non Conformity**	**Recommendations**	**Risk Level**	**Location**	**Required Completion Date**	**Person/s Responsible**	**Progress/Comments**	**Date Completed**
Are house keeping arrangements satisfactory?	An area of concern was the overall condition of the staff work room on the 3rd Floor which was untidy with significant amounts of combustible materials poorly situated.	The poor housekeeping here could result in greatly assisting fire spread should one occur therefore a general clean up is required.	Low	Staff workrooms and offices	17/05/2022	Management / Lecturing staff	Management to instruct faculty staff to clear their individual areas.	Ongoing
Category 5: Means of Escape								
Question	**Non Conformity**	**Recommendations**	**Risk Level**	**Location**	**Required Completion Date**	**Person/s Responsible**	**Progress/Comments**	**Date Completed**
Do the fire resisting door sets meet the appropriate standard?	Ineffective self closing devices.	Repair or replace the self-closing device/s to ensure fire door/s close fully into their frame/s against the door stops.	Medium	First Floor Corridor	18/03/2022		Parts are on order. Estimated repair to be carried out on the 4th April 2022.	
Do the fire resisting door sets meet the appropriate standard?	The intumescent cold smoke seals installed to prevent the spread of smoke and fire between compartments are missing.	The missing intumescent cold smoke seals must be replaced to ensure that the spread of smoke and fire is restricted.	Medium	G06	18/03/2022	Estates	The seal is not missing and will still work if there is a fire. The small soft insert has been ordered. 22.03.2022	
Category 7: Fire Detection and Warning								
Question	**Non Conformity**	**Recommendations**	**Risk Level**	**Location**	**Required Completion Date**	**Person/s Responsible**	**Progress/Comments**	**Date Completed**
Is the fire alarm system routinely tested, inspected	No up to date record of inspection and maintenance in accordance with BS 58391.	The fire alarm system must be inspected and maintained by a competent certificated organisation in accordance with BS 58391.	Medium	Ground floor	18/03/2022	Estates / Securigroup	Estates test the system weekly and Securigroup maintain the system. Copy of contract uploaded to electronic logbook.	22.03.2022

and maintained in accordance with current guidance?								
Category 8: Emergency Lighting								
Question	**Non Conformity**	**Recommendations**	**Risk Level**	**Location**	**Required Completion Date**	**Person/s Responsible**	**Progress/Comments**	**Date Completed**
Is the emergency lighting system routinely tested, inspected and maintained in accordance with current guidance?	Not inspected and maintained in accordance with BS 52668.	The emergency lighting system must be inspected and maintained by a competent certified organisation in accordance with BS 52668.	Medium		18/03/2022	Thomas Smith Electrical	The whole system is checked on a four year rotation, meeting with the regulations. Checks are completed monthly, annually & 5 yearly.	22.03.2022
Is the emergency lighting system routinely tested, inspected and maintained in accordance with current guidance?	No monthly emergency lighting tests are recorded.	The emergency lighting system should be tested monthly and records maintained, in accordance with BS 52668.	Medium		18/03/2022	Thomas Smith Electrical	Al lighting tests are recorded. Last paperwork uploaded to the electronic logbook.	22.03.2022
Category 10: Management								
Question	**Non Conformity**	**Recommendations**	**Risk Level**	**Location**	**Required Completion Date**	**Person/s Responsible**	**Progress/Comments**	**Date Completed**
Have employees received appropriate fire safety awareness training?	Fire marshals/wardens training overdue.	Employees expected to fulfil a role of a fire marshal/warden will require comprehensive training from a competent person/organisation to cover all of their additional responsibilities. It should be remembered that for each fire marshal/warden required a deputy should be trained to cover any absences. In addition, a fire marshal/warden should take no longer than one minute to search a designated area.	Medium		18/03/2022	H&S Manager	**Training will be scheduled prior to the Summer break.**	
Are house keeping arrangements satisfactory?	Inappropriate use of rooms/space.	The room/space should be utilised for the purpose for which it was designed.	Medium		18/03/2022	Faculty housekeeping		
Are house keeping arrangements satisfactory?	The furniture and furnishings present is not compliant with current standards and/or damaged thereby exposing its foam interior.	The noncompliant/damaged furniture/furnishings should be removed or repaired to ensure compliance with the Furniture and Furnishings (Fire) (Safety) Regulations 1988 as amended.	Low	Common room	17/05/2022	Students Association / Estates	The room has been taken out of use and the furniture has now been removed for disposal.	22.03.2022

Campus:	Springburn							
Category 2: Sources of Ignition								
Question	**Non-Conformity**	**Recommendations**	**Risk Level**	**Location**	**Required Completion Date**	**Person/s Responsible**	**Progress/Comments**	**Date Completed**
Are all electrical installations and appliances correctly installed and maintained?	There is unsafe use of extension leads.	These appliances are to be used in accordance with manufacturers' instructions or alternatively, additional power sockets provided in this area. Daisy chain	Low	432	17/05/2022	Finance Staff	In progress (Desk area has insufficient floor plug blocks to accommodate 4 working desks - MT met with I Gordon who will ask the electrician to look at this area)	Ongoing
Category 3: Sources of Fuel								
Question	**Non-Conformity**	**Recommendations**	**Risk Level**	**Location**	**Required Completion Date**	**Person/s Responsible**	**Progress/Comments**	**Date Completed**
Are house keeping arrangements satisfactory?	The standard of housekeeping regarding combustible materials in the staff work area is inadequate.	Ensure adequate storage areas are provided and that housekeeping within these areas is of an acceptable standard.	Medium	Staffrooms	18/03/2022	Teaching Staff	Have been notified to clear	Ongoing
Category 5: Means of Escape								
Question	**Non-Conformity**	**Recommendations**	**Risk Level**	**Location**	**Required Completion Date**	**Person/s Responsible**	**Progress/Comments**	**Date Completed**
Do the fire resisting door sets meet the appropriate standard?	Fire doors are fouling against the frame/dragging on the floor surface and are not closing completely against the door stops.	All fire doors and associated self closing devices should be maintained to ensure they close fully into their frames.	Medium		18/03/2022	Joiner Technician	Ongoing	
Do the fire resisting door sets meet the appropriate standard?	Ineffective self closing devices.	Repair or replace the self closing device/s to ensure fire door/s close fully into their frame/s against the door stops.	Medium		18/03/2022	Joiner Technician	Ongoing	
Do the fire resisting door sets meet the appropriate standard?	The fire doors have a large gap between the doors and the frame which may prevent the intumescent seals being effective.	The doors should be adjusted to ensure that there is no more than a 3mm gap between the hinge edge, leading edge and the top of the door frame.	Low	Ground Floor Music Corridor	17/05/2022	Joiner Technician	Ongoing	
Do the fire resisting door sets meet the appropriate standard?	It was noted during the visit that there were several issues regarding the proper function of fire doors and these are highlighted in the action plan.	It is vital that fire doors operate correctly, especially those surrounding the atrium therefore a regular inspection regime should be set up and any defects corrected.	Medium		18/03/2022	Joiner Technician	Ongoing	
Are house keeping arrangements satisfactory?	Combustible materials are located/stored in the escape routes.	Items that are a source of fuel or are combustible and likely to increase the fire loading or spread of fire, should not be located on any corridor, stairway or circulation space that will be used as an escape route. Therefore, the combustible materials stored in the escape routes must be removed.	Medium		18/03/2022	Estates	Tiles removed	2/03/22

Question	Non-Conformity	Recommendations	Risk Level	Location	Required Completion Date	Person/s Responsible	Progress/Comments	Date Completed
Are house keeping arrangements satisfactory?	The escape route is obstructed.	The items obstructing the escape route must be removed immediately.	Medium	Student Hub ground floor	18/03/2022	Estates	Area out of bounds to all staff and students	16/02/2022
Category 7: Fire Detection and Warning								
Question	**Non-Conformity**	**Recommendations**	**Risk Level**	**Location**	**Required Completion Date**	**Person/s Responsible**	**Progress/Comments**	**Date Completed**
Is there an adequate method for raising the alarm and detecting a fire present in the premises?	Manual call point damaged in games room	Contractor to be contacted to repair manual call point. The MCP should be protected against impact damage in this area.	Low	Games Hall ground Floor	17/05/2022	CHUBB Fire	Call point has been replaced	3/3/22
Category 8: Emergency Lighting								
Question	**Non-Conformity**	**Recommendations**	**Risk Level**	**Location**	**Required Completion Date**	**Person/s Responsible**	**Progress/Comments**	**Date Completed**
Is the emergency lighting system routinely tested, inspected and maintained in accordance with current guidance?	No record of annual inspection and maintenance in accordance with BS 52668.	The emergency lighting system must be inspected and maintained by a competent certified organisation in accordance with BS 52668.	Medium		18/03/2022	Tommy Smith	The whole system is checked on a four year rotation, meeting with the regulations. Checks are completed monthly, annually & 5 yearly.	Ongoing
Category 10: Management								
Question	**Non-Conformity**	**Recommendations**	**Risk Level**	**Location**	**Required Completion Date**	**Person/s Responsible**	**Progress/Comments**	**Date Completed**
Have employees received appropriate fire safety awareness training?	Fire marshals/wardens training overdue.	Employees expected to fulfil a role of a fire marshal/warden will require comprehensive training from a competent person/organisation to cover all of their additional responsibilities. It should be remembered that for each fire marshal/warden required a deputy should be trained to cover any absences. In addition, a fire marshal/warden should take no longer than one minute to search a designated area.	Medium		18/03/2022	Geoff Lawson	Training will be scheduled prior to the Summer break.	Ongoing
Are house keeping arrangements satisfactory?	The furniture and furnishings present is not compliant with current standards and/or damaged thereby exposing its foam interior.	The noncompliant/damaged furniture/furnishings should be removed or repaired to ensure compliance with the Furniture and Furnishings (Fire) (Safety) Regulations 1988 as amended.	Low	1st floor bridge between main building and workshops	17/05/2022	Estates	Sofa removed and disposed	11/03/22

Campus:	West							
Category 2: Sources of Ignition								
Question	**Non-Conformity**	**Recommendations**	**Risk Level**	**Location**	**Required Completion Date**	**Person/s Responsible**	**Progress/Comments**	**Date Completed**
Are all heating appliances correctly installed, adequately protected and maintained?	There is no record of appropriate servicing and maintenance of the gas appliances.	Gasfired boilers and other appliances, should be subject to periodic inspection and maintenance by a competent Gasafe engineer in accordance with the Gas Safety (Installation and Use) Regulations 1998 (GS(IU)R 98). Records are to be maintained.	Medium		18/03/2022	G Lawson	Records of boiler maintenance are kept in the Estates office for viewing. Richard Irvin FM Limited are the company who carry out all boiler maintenance	23/02/2022
Are all electrical installations and appliances correctly installed and maintained?	There is unsafe use of extension leads.	These appliances are to be used in accordance with manufacturers' instructions or alternatively, additional power sockets provided in this area.	Medium		18/03/2022	E McWilliam	Extension cable has been removed	23/02/2022
Category 7: Fire Detection and Warning								
Question	**Non-Conformity**	**Recommendations**	**Risk Level**	**Location**	**Required Completion Date**	**Person/s Responsible**	**Progress/Comments**	**Date Completed**
Is the fire alarm system routinely tested, inspected and maintained in accordance with current guidance?	No record of inspection and maintenance in accordance with BS 58391.	The fire alarm system must be inspected and maintained by a competent certificated organisation in accordance with BS 58391.	Medium		18/03/2022	G Lawson	Chubb Fire services inspect our system on a 25% scale per visit x4 per year. all records are kept for viewing in our Campus Office.	17/02/2022
Category 8: Emergency Lighting								
Question	**Non-Conformity**	**Recommendations**	**Risk Level**	**Location**	**Required Completion Date**	**Person/s Responsible**	**Progress/Comments**	**Date Completed**
Is there an adequate method for illuminating the escape route and safety equipment in the premises?	The existing escape lighting system is damaged/defective. No visible charging light.	A competent person is to survey the existing system and repair/replace luminaries as required.	Medium		18/03/2022	Estates	**Requires survey by electrician**	
Is the emergency lighting system routinely tested, inspected and maintained in accordance with current guidance?	No monthly emergency lighting tests are recorded.	The emergency lighting system should be tested monthly and records maintained, in accordance with BS 52668.	Medium		18/03/2022	G Lawson	Monthly tests are carried out, Records kept in campus office for viewing.	09/03/2022
Category 10: Management								
Question	**Non-Conformity**	**Recommendations**	**Risk Level**	**Location**	**Required Completion Date**	**Person/s Responsible**	**Progress/Comments**	**Date Completed**
Are management and employees fully aware of the fire safety features provided and their purpose?	The record of the maintenance of fire safety measures was not kept up to date.	A fire precautions logbook is provided and should be maintained to include details of fire instructions, fire training, fire drills; and testing, inspection and maintenance of alarm and detection systems, portable firefighting equipment, fixed firefighting installations and emergency lighting systems.	Medium		18/03/2022	G Lawson	Logbook has been updated for viewing.	18/03/2022

Question	Non-Conformity	Recommendations	Risk Level	Location	Required Completion Date	Person/s Responsible	Progress/Comments	Date Completed
Have employees received appropriate fire safety awareness training?	Fire marshals/wardens training overdue.	Employees expected to fulfil a role of a fire marshal/warden will require comprehensive training from a competent person/organisation to cover all of their additional responsibilities. It should be remembered that for each fire marshal/warden required a deputy should be trained to cover any absences. In addition, a fire marshal/warden should take no longer than one minute to search a designated area.	Medium		18/03/2022		Training will be scheduled prior to the Summer break.	

Date of Incident	11 March 2022	**Report No.**	001-2022

RIDDOR reportable?	Yes ☒ No ☐	**Ref No.**	DangerOcc-8C135E011C - submitted 14 March 2022

Investigation Team	Geoff Lawson, Health & Safety Manager	**Signature(s)**	
	Peter Brown, Director Planning, Performance & Curriculum		
		Date	

Summary of Investigation Findings
The summary should outline the event(s), who was involved, what happened, the scope of the investigation, the analysis and outcomes and any recommendations to prevent or minimise the recurrence of the accident / incident.
At approximately 8:55am on Friday 11th March 2022, Iain Baird (IB, Jewellery Technician, BCDI Faculty) opened the door from the second floor corridor into Room 213 (Jewellery Workshop) at Springburn Campus (see Documents - D25). He immediately noticed a 'bleach-like' smell and on entering the room to investigate noticed fumes eminating from a small metal cabinet (see Documents - D3) located by the window. Shortly after, his line-manager David Webster (DW, Curriculum Manager, BCDI Faculty), arrived on scene and took charge of the incident. Kathleen Duncan (KD, Jewellery Lecturer) was sent to first floor science technicians office (room 120) to seek assistance from Elaine MacDougall (EM, Senior Science Technician, ECS Faculty) for a suspected Nitric Acid leak in the Jewellery Workshop. EM collected a spillage kit and a large quantity of Sodium Hydrogen Carbonate (commonly known as baking soda or bicarbonate of soda) to neutralise the suspected Nitric Acid. EM and KD returned up the stairs to the second floor and as they opened the door were met with an acrid smell. EM attempted to enter Room 213 but decided that the fumes were too great and that a suitable mask or respirator was required. EM instructed the Jewellery staff to evacuate the adjoining room (215) and close the fire doors to contain the fumes. EM and KD then went to reception to meet Graham Phee (GP, Senior Facilties Officer, Estates and Facilities Department) in order to find some respirators. None where found and EM and GP then returned to Room 213 with FP3 face-masks. On return to the second floor it was apparent that the fumes were very strong and EM suspected that the incident was becoming more serious. On re-entry to room 213, fumes were visible eminating from the small metal cabinet next to the windows. GP could feel a stinging sensation on his lips and tongue through the FP3

mask and following a short breather outside in the corridor, returned to the cabinet to assist EM.

EM attempted to neutralise the 'acid' with the Sodium Hydrogen Carbonate, but because of the location of the tray of chemicals in the cupboard was unable to 'dump' the quantity required to achieve this. Aware that the FP3 maks were probably inadequate EM realised that time was running out before putting herself at risk.

She noticed quite a large volume of liquid in the tray but did not attempt to lift it out of the cabinet. She was not able to determine what type of chemical had leaked or what chemical it was reacting with.

At this point they both returned to the corridor to consult and EM advised GM that the Scottish Fire and Rescue Service (FRS) should be contacted for advice and assistance and to evacuate the building.

On their way back to reception, GP swiftly briefed senior management on the incident before returning to the Facilities office to phone Springburn Fire station, which he did at 9:18am. The Fire Officer at the stations advised GP to dial 999, as this would ellicit a more comprehensive, risk-based response. He called 999 at 9:21am and on completion of the call, activated the call point to evacuate the building at 9:24am.

The FRS arrived at Springburn Campus at 9:28am

As the FRS Incident Commander debussed, Derek Smeall (DS, Principal) approached and passed on the information that had been relayed to him by GP. He then beckoned over DW who provided a more detailed explanation of the incident.

After approximately one hour, Senior Management began to direct staff and students, who were able to leave the site, either for home or another campus.

Up to this point it was still believed that a 2 litre bottle of Nitric Acid had leaked and was emiting fumes and there were other unidentied containers within the same cabinet

It was subsequently determined that the cause of the fumes was a chemical reaction between 'Lacomit' Remover and 'Lacomit' Varnish, stored in two corroded containers held within the small metal cabinet in Room 213 (see Documents - D4)

Approximately two hours into the incident the FRA Incident Commander informed the Principal that:

- there was a lack of clarity around the bottles found in the vicinity
- some chemicals in the immediate vicinity were stored in 'vinegar and coca-cola bottles'
- in his opinion, chemical storage was of a standard that was "not acceptable"
- a report would be made to the Health and Safety Executive (HSE)

FRA operations, including specialist continued throughout the day and resulted in the small metal cabinet and content being removed from the room to an external place of safety at the back of the campus (the content in a large COSHH locker (see Documents - D1 & D2) and the cabinet in the gas bottle storage area (D3). All content were made safe before removal from the building and will all be permanently disposed of in accordance with current regulations.

At approximately 3pm the FRA had completed operations on campus and departed.

At an urgent SMT meeting convened by the Principal at 9am on Monday 14th March, the Health and Safety Manager (Geoff Lawson) and the Director Planning, Performance & Curriculum were verbally directed to commence a full investigation into all circumstances leading up to, during and after the incident at Glasgow Kelvin College's Springburn Campus

on the morning of Friday 11th March 2022. A follow-up email from the Principal formalisied this directive (see Documents - D26). A RIDDOR report was submitted to HSE on Monday 14th March 2022 (see Documents D24)

Investigation Analysis	
What was / were the event(s) which contributed to the accident / incident?	1. Cabinet containing COSHH material (including 'Lacomit' Varnish and Remover) used by staff member who left the college on 29 September 2015. Materials had lain undisturbed in the interveneing 6 and a half years. 2. 'Lacomit' product containers had deteriorated over time, such that the leaks substances reacted causing the fumes noted during the incident 3. COSHH forms (Safety Data Sheets and Assessments) for products held in cabinet were not present as these had not been identified as present on campus in the departmental inventory 4. Departmental staff's unfamiliarity with historically stored COSHH items and unused storage furniture 5. Safety inspection form (HS002) contains inadequate COSHH review process
What was / were the identified or possible cause(s) of the accident / incident?	1. A 'personal' cabinet used to store COSHH materials which were then not disposed of following that staff members departure in 2015. 2. Inadequate College-wide and departmental COSHH internal audit and review process 3. Incomplete safety inspection process which failed to identify unused, undisturbed COSHH materials 4. Absence of a comprehensive procedure clearly identifying differing COSHH hazards (oxidising, flammable etc) and ensures a safe, hazard specific and adequate storage solution in accordance with COSHH regulations 5. Absence of documented departmental COSHH roles and responsibilities 6. Lack of familiarity/clarity of content of all departmental storage
Which of the identified or possible cause(s) is / are within the control of the workplace?	1. Use of 'personal' storage for COSHH items. 2. Robust 'off-boarding' process for staff departure 3. Internal and external COSHH audit and review processes 4. Storage procedures (which clearly identify differing COSHH hazards (oxidising, flammable etc) and ensures a

	safe, hazard specific and adequate storage solution in accordance with COSHH regulations) 5. Roles and responsibilities 6. Inventory review
What corrective action(s) / solution(s) could be implemented to eliminate or reduce the risk of the identified cause(s)?	See recommendations

Investigation Outcomes	
Outline any controls that were put into place immediately after the accident / incident to eliminate or reduce the risk of recurrence of the incident. (Outline the controls and who was responsible for implementing them).	
Control measures immediately implemented	1. All materials/substances involved in incident made safe and removed from building by FRS 2. All departments and faculties directed to conduct immediate review of their COSHH inventories and storage solutions 3. Deadline for legally mandated training advanced from 30 March 2022 to 20 March 2022 4. WorkRite COSHH module made available to additional staff 5. Six respirators ordered to enhance emergency response 6. Communication to all staff advising of incident and subesquent actions taken 7. RIDDOR report submitted
Name(s) of person(s) who implemented them.	Geoff Lawson in coordination with Senior Management Team

Recommendations
Outline recommended corrective action(s) (i.e. solutions) to prevent the recurrence of the accident / incident (number the recommendations from the most effective to the least effective i.e. Hierarchy of Controls).
1 Identify all staff with exposure or potential exposure to COSHH materials in the course of their duties and provide immediate access to the WorkRite COSHH module 2 College-wide review of ALL COSHH materials held. Rationalise requirements and stocks 3 All faculites and departments to review COSHH inventories, rationalising their requirements and stocks held 4 All faculties and departments review their storage processes and update to College best practice (colour coded, hazard specific and iaw COSHH regulations) 5 Following faculty and departmental inventory reviews, dispose of all excess, out of date or no longer required stock arranging a college-wide waste uplift 6 Review adequacy of all COSHH storages, enhancing or replacing as necessary 7 Consider provision of a purpose-built storage area for all chemicals located outside each building with one person having overall control 8 Set up central COSHH inventories for each campus, stating exact quantities, locations of all hazardous substances - live documents for easy editing (potential for use of CMS as method) 9 Draft plans of all rooms containing COSHH materials/substances, posting completed plan on the outside of relevent storage or work area. Duplicate copies to be provided to a Master log held at each campus reception for use by FRS in an emergency. Plans should contain storage layout etc, specific hazards (flammable etc.), approximate quantities, specific emergency actions (as per SDS) 10 As a matter of urgency nominate a 'COSHH Custodian' for each Faculty and Department 11 Provide immediate internal training for each nominated 'COSHH Custodian' covering revised and updated college COSHH ordering, storage, use and disposal procedures 12 In addition, provide 'COSHH Custodians' with immediate access to specific external COSHH qualification course with set expectation for training to be completed within four weeks 13 Where relevant replace any metallic COSHH locker trays with impermeable ones 14 Review, update and communicate college COSHH emergency procedures 15 Provide emergency respiratory equipment to Springburn and East End campuses (to be reviewed on completion of inventory reviews at ALL campuses) providing relevant training for identified staff (COSHH Custodians, Estates Staff, Managers etc.) 16 With immediate effect implement twice-annual internal Safety inspection/COSHH audits 17 On completion of implementation of recommendations 1 to 16, engage external subject matter expert (SME) to conduct full audit of College COSHH procedures

18 As a matter of urgency implement any additional recommendations subsequently received from the Health and Safety Executive (HSE)

19 On completion of external COSHH audit, engage external SME to conduct full H&S Management audit

20 Nominate one Fire Warden to meet FRS crew on arrival, escorting them into the buidling and direct them to the Evacuation Controller

21 Add an additional prompt to Evacuation Checklist to ensure adequate cogniscience of evacuee welfare, including deferral to Senior Management after 1 hour

22 Update the incident report form (HS001) to include section for COSHH/spillages etc.

23 Investigate transition to 'Just in time' COSHH inventories - buying when required and disposing of what's not needed?

24 Investigate feasibility of promotion of Techician to Senior Technician (COSHH Custodian) (Peter?)

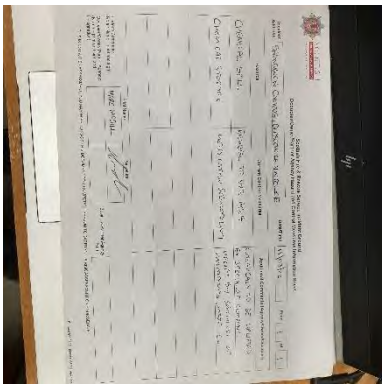
25 Outright ban on COSHH storage in anything other than a designated COSHH locker (no personal holdings)

26 Ensure all COSHH materials/substances are contained within proprietary containers (i.e. no coca cola or vinegar bottles etc)

27. Safety Inspection Form (HS002) needs to be amended to enhance COSHH review process

28. All lockers should be labelled accurately. All non-COSHH lockers to be clearly marked 'COSHH FREE'

Additional Information and Notes
N/A

Evidence (specify / attach as appropriate)		
Photographs or sketches of the scene	1.	2.
	3.	4.
	5.	6.
		

Physical items (e.g. equipment, parts, fragments, substances)	COSHH items from incident awaiting disposal
Clinical (e.g. samples of breath, urine or blood)	Not applicable
Environmental (e.g. samples from air, water, soil)	Not applicable
Documents	D1. Photo 20220314_134155. Content of cabinet D2. Photo 20220314_134200. Content of cabinet, wide angle. D3. Photo 20220314_153656. Metal cabinet and additional content. D4. Photo 'Lacomit' containers D5. Fire Service Information Sheet D6. Photo Fire and Rescue Incident Commanders notebook D7. BDCI Safety Inspections 2014-2019 D8. Safety Inspection 23 February 2015 D9. Safety Inspection 30 November 2015 D10. Safety Inspection 4 March 2016 D11. Safety Inspection 20 May 2016 D12. Safety Inspection 10 June 2016 D13. Safety Inspection 26 October 2016 D14. Safety Inspection 21 October 2017 D15. Safety Inspection May 2018 D16. Safety Inspection September 2018 D17. Safety Inspection December 2018 D18. Safety Inspection April 2019 D19. Safety Inspection October 2019 D20. Safety Inspection March 2020 D21. Safety Inspection November 2020 D22. Safety Inspection 22 October 2021 D23. Scottish Fire and Rescue Service Incident Ground Occupier/Owner/Partner Agency Hazard and Control Measures Information Sheet dated 11 March 2022 D24. RIDDOR Report - DangerOcc-8C135E011C, date 11 March 2022 D25. PowerPoint Floor Plan D26. email H&S Incident of 11 March 22 investigation

	D27. Incident Report Form (HS001) D28. Safety Inspection Form (HS002) D29. Health and Safety Control Manual (HSCM) Section 9.7 - COSHH
Data print outs	DP1. COSHH Management System (CMS) Jewellery CMS_Inventory 11 March 2022 DP2. CMS User_Stats dated 16 March 2022 DP3. Public Health England Nitric Acid Toxicological Overview DP4. 'Lacomit' Remover SDS_printed 14 March 2022 DP5. 'Lacomit' Varnish SDS_printed 14 March 2022 DP6. David Webster WorkRite Training Summary @ 11 March 2022 DP7. Gordon Stewart WorkRite Training Summary @ 11 March 2022 DP8. Iain Baird WorkRite Training Summary @ 11 March 2022 DP9. James Davidson Workrite Training Summary @ 11 March 2022 DP10. Kathleen Duncan WorkRite Training Summary @ 11 March 2022
CCTV footage	None available
Interviews (person / people involved and witnesses)	WS1. Witness Statement Graham Phee WS2. Witness Statement Elaine MacDougall WS3. Witness Statement Iain Baird WS4. Witness Statement David Webster WS4a. Initial Report David Webster WS5. Witness Statement Derek Smeall WS6. Witness Statement Grant McAleese WS7. Witness Statement Andy Allan WS8. Witness Statement Steven Crawford

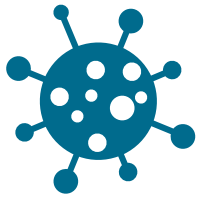
Fraud and irregularity 2020/21

Sharing risks and case studies to support the Scottish public sector in the prevention of fraud

AUDIT SCOTLAND

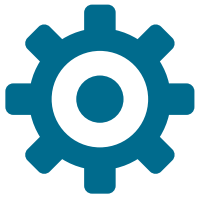
Prepared by Audit Scotland for public bodies and auditors
July 2021

Key messages



1. Significant challenges due to Covid-19

Since the start of 2020/21, the Covid-19 pandemic and the associated lockdowns have brought significant challenges across the public sector. Public bodies have sought to continue to deliver services in new working environments while at the same time experiencing an increase in demand for many services. The challenges during the last year include additional fraud risks for public bodies to identify and manage.



2. Wide range of action required to mitigate new risks

The new fraud risks cover a variety of areas. This means a wide range of actions are required by public bodies to attempt to mitigate these risks.

3. Weaknesses in controls contribute to fraud and irregular activities

Weaknesses in controls have contributed to a variety of fraud and irregular activities being identified across the Scottish public sector. During 2020/21, external auditors reported 13 cases of fraud and irregularity valued at £0.4 million. The value of reported fraud and irregularity remains small compared to the 2020/21 annual Scottish budget of £49 billion.

4. Counter-fraud hub

Audit Scotland's counter-fraud hub contains useful counter-fraud information.

Recommendations

Public bodies should ensure good governance and counter-fraud arrangements are in place, including:

- having in place appropriate governance and oversight arrangements for counter-fraud
- regularly reviewing controls and governance arrangements to ensure they remain fit for purpose
- being alert to emerging fraud risks and where appropriate working with others to help alleviate these risks
- considering whether appropriate controls are in place to prevent the risks identified in this report materialising in their own organisation
- considering whether the weaknesses in internal control that facilitated each case of fraud or irregularity identified in this report may also exist in their own organisations, and taking the required corrective action.

Auditors should confirm that:

- appropriate governance arrangements for the prevention and detection of fraud are in place at their audit clients and that appropriate reviews and amendments of controls have taken place in response to new ways of working
- internal controls at their audit clients are sufficiently strong to prevent the types of fraud and irregularity highlighted in this report.

Background

Impact of Covid-19

The risk of fraud and error has increased over the last year due to the Covid-19 pandemic. This is due to many reasons, including:

- public bodies have become stretched, controls and governance arrangements have required to be changed
- staff working remotely and under pressure
- staff adapting to new ways of working with associated new processes and procedures
- staff being redeployed to work in new and unfamiliar departments as public bodies have responded to increased demands for certain services
- continuous fraud attempts on public bodies including both traditional types of fraud and newer cybercrimes
- former verification and control processes being unable to operate as new ways of working are introduced
- new support schemes for business and communities being developed and implemented at speed.

Public bodies need to review their systems and identify areas where the threat from fraud and error has increased. They need to review existing controls to ensure they are still effective and appropriate and at the same time introduce new controls to address new risks. Measures like these have always been important but the unprecedented challenges and pressures brought by the pandemic, and the opportunities it has presented for fraudsters, bring a renewed focus on ensuring effective governance and controls are in place.

Additional risks will continue to emerge as public money and services are targeted by fraudsters. Fraudsters will continue to look for new opportunities to exploit weaknesses in systems and controls. Public bodies and auditors should stay alert to new scams and approaches by fraudsters, and regularly review controls and governance arrangements to ensure they remain fit for purpose.

Good governance and sound controls are essential in crisis and changing situations.

Aims of this report

This report sets out a range of fraud risks emerging since the start of the Covid-19 pandemic along with suggestions of what public bodies may do to help reduce these risks. It aims to help public bodies identify and manage these risks.

This report also shares information about cases where internal control weaknesses in public bodies have led to fraud and irregularity, to help prevent similar circumstances happening again. External auditors have shared specific details about significant frauds and other irregularities in public bodies during 2020/21. The level of fraud and irregularity reported by external auditors of £0.4 million remains small compared to the 2020/21 Scottish budget of £49 billion.

This report is informed by information provided by external auditors during 2020/21 in their fraud and irregularity returns to Audit Scotland. External auditors are required to report frauds (or suspected frauds) where they are caused or facilitated by weaknesses in internal controls at public bodies. Frauds and irregularities are considered significant where the value of the loss is over £5,000 or where it is of significance due to the nature of the activity.

Auditors of local authorities are not required to report cases of fraud perpetrated by claimants, for example, grant claimants or housing benefit claimants, unless the fraud was facilitated by the collusion of local authority staff or otherwise by weaknesses in internal control. The cases included in this report are likely to have been investigated internally, but it is not necessary for the police to have been involved or for it to have been proven as fraud in a court of law.

Key fraud risks identified in 2020/21

We have grouped the fraud-related risks identified by external auditors over the last year into the following seven categories. They include, but are not limited to, risks associated with:

1. Covid-19 funding and reopening of premises and services

2. Health and wellbeing

3. IT and cybercrime

4. Governance

5. Procurement

6. Payment

7. Payroll and recruitment

1. Covid-19 funding and reopening of premises and services

- Government stimulus packages to support individuals and businesses are provided quickly, possibly with a lower level of scrutiny and due diligence than has previously been in place. Often the support is provided to people and businesses that the public body had no previous relationship with, making the verification of details more difficult.
- Councils may receive emails or Freedom of Information requests asking for details about property details, reference numbers or business grant applications. Fraudsters are possibly looking to identify eligible businesses that have not applied for grants, with a view to submitting a fraudulent application.
- Councils may receive requests for business rate liabilities to be changed. This may be an attempt to ensure a business falls within a category qualifying for grants.
- Due to applications for Covid-19 related support being made online, there is a risk that fraudulent documents and details are provided.
- Councils may receive fraudulent applications for funding purporting to be from genuine qualifying businesses. These applications are often supported by what appears to be genuine supporting information which has often been obtained from publicly available sources.
- As buildings and offices reopen, emails may be received purporting, for example, to be from the Health and Safety Executive (HSE) saying the HSE is carrying out Covid-19 spot checks on newly opened premises. A link supposedly to guidance documents leads to a file which contains malicious software (malware).
- Texts may be received advising recipients that they are eligible for a Covid-19 grant and that an attached form requires to be completed. The form contains a link to a scam website, possibly similar to the HMRC website, asking for business, personal and bank details.

Additional Covid-19 related risks:

Covid-19: Emerging fraud risks

July 2020

2. Health and wellbeing

- Remote working may result in isolation and/or mental health issues. This may lead, in some cases, to increased addictive behaviours (eg, gambling), which could result in vulnerability to serious organised crime gangs.
- An increase in internal fraud in public bodies is possible as staff and their families are under increased levels of financial and health pressures.
- Working for sustained periods of time at high levels of demand may lead to errors or fraud due to lapses in concentration.
- Staff/volunteers could take advantage of vulnerable service users, for example by gaining access to bank cards, cash drop-offs at client's house and befriending with sinister intentions.
- Emails may be received purporting to be from the NHS offering a Covid-19 vaccination. Recipients are requested to provide bank details.

3. IT and cybercrime

- Staff working remotely may pose potential security risks, eg when using personal devices and/or using removable devices to download data.
- Household members may gain unauthorised access to confidential information such as payroll, social work client details etc, by looking at screens or documents used by staff.
- Staff may be more likely to be tempted to steal data when working remotely without the normal office supervision.
- Staff working remotely may receive calls from fraudsters claiming to be legitimate technical support services and attempting to gain access to systems. The callers may say that they are looking at issues with the public body's network and will request the staff member's login details in order to 'fix' the system issue.
- Staff working at home may receive calls purportedly from their broadband providers. The caller says that they are having technical problems with the service. The caller asks the recipient to switch on their computer to check the broadband signal strength and then to enter a scam web address and/or download a piece of malware.
- There is a risk of increased cybercrime as more public-sector staff connect remotely to access systems and for meetings using online video conference services.
- There is a risk of more system-access breaches where personal information is accessed without a valid reason by staff working remotely, eg possibly to check friends' applications for services.
- It is easier for fraudsters to send 'urgent' emails or texts pretending to be from senior members of staff to their under-pressure teams asking for money to be transferred or for information to be disclosed.
- There is a risk of ransomware attacks. This is where malware is put into bodies' systems and leaves a ransom note demanding money in exchange for the return of information or the reinstatement of systems.
- There is a risk of an increase in **phishing** emails trying to get staff working under pressure to click on links which allow fraudsters access to public-sector systems. For example, staff receive scam emails inviting them to a video conferencing meeting, supposedly being held by someone they know and trust. The link provided leads to a fraudulent log-in page, which asks for the recipient's username and password.

Phishing:

Where criminals send emails purporting to be from reputable sources in order to deceive individuals into providing information or data such as passwords, user names or bank details, or to click on a link that allows malware to be downloaded.

4. Governance

- Public-sector staff are working under extreme pressure which may mean some internal controls are suspended or relaxed.
- Existing controls may have been relaxed to assist homeworking for staff and access to services for clients.
- Fraud investigations may be paused or unable to continue due to difficulties in collecting evidence or investigation staff being redeployed to frontline services.
- When buildings are closed there are additional risks to the security and unauthorised use of assets from both internal and external sources as the removal or unauthorised use of assets may go undetected.
- New equipment and IT devices purchased during the pandemic may be at more risk of being lost or stolen due to possible weakness in controls around delivery, asset-tagging and recording in asset registers when staff are working from home. Any losses may not be detected.
- Staff may be transferred from their own departments to other areas to meet increased demand for certain services. This may leave some departments under-staffed at the same time that inexperienced staff may be working remotely without a full understanding of the required procedures and controls.
- There is a risk of weakened governance arrangements as internal audit teams are redeployed to operational areas.

5. Procurement

- Previous controls may be relaxed to allow bodies to buy new or existing goods or services which are required urgently, possibly from new suppliers.
- Fraudsters may be 'selling' popular and/or hard-to-get items online. The products may not arrive or may be counterfeit, eg medicines, personal protective equipment (PPE) such as face masks and gloves, and hand sanitiser products which do not provide the necessary level of protection.
- An increase in medical and sanitary waste may see criminals attempt to gain waste management contracts. This could result in the inadequate disposal of the waste, with the potential associated harm to public health as well as generating proceeds for the criminals.
- Bodies may buy goods/services from companies without due diligence and vetting being completed due to the urgent demand. This increases the risk of collusion between companies, eg bid fixing, and between companies and staff in the public body buying the goods/services.
- Bodies may receive texts or phishing emails purporting to be delivery companies saying that a parcel is awaiting delivery but that an unpaid shipping fee must be paid. The texts and emails include a link to a scam website asking for payment details.
- Bodies may also receive texts or phishing emails purporting to be from delivery companies saying that they tried to deliver a parcel to closed offices. A link is provided purporting to allow the rescheduling of the delivery. The link leads to a scam website asking for contact and payment details.

6. Payment

- Mandate and diversion fraud may increase as fraudsters try to get employees to update suppliers' bank details and make payments as soon as possible, knowing staff are under pressure. Some attempts may be made using a compromised email account of a genuine member of staff employed at either the public sector body or in an existing supplier.
- Due to staff working from home and under pressure, duplicate payments are possibly not detected, or payments may be made without checking whether goods and services were received to a satisfactory quality.
- Due to controls being loosened it may be possible for staff to pay invoices above their authorisation limits or without the normal approvals.
- Emails may be received from fraudsters purporting to be from a senior member of staff in a contractor requesting copies of initial contracts/award letters and previous invoices last issued. The fraudulent email may also note there has been a change in their bank account details.
- Public bodies may be contacted by someone purporting to be from the fraud department at the body's bank and advising of attempted frauds made against the body's bank accounts. The fraudster then may persuade the member of staff that that they can stop the fraud by setting up a payment to a given sort code and account number.
- Messages may be received purporting to be from the bank saying that a request to add a new payee has been set up. The recipients are asked to click on a link to authorise or cancel this request. The link leads to a scam website which asks for bank account details.
- Messages may be received purporting to be from a known supplier advising that an unexpected sum of money will be debited from the body's bank account. The recipient is asked to click a link to a scam website supposedly in order to cancel the payment.
- Emails may be received where a fraudster tricks officers into thinking a message came from a person they know. For example, a staff member may receive an email from what appears to be a senior colleague requesting the purchase of gift cards and for the cards and codes to be emailed by return email, or that certain invoices have been authorised for payment.

7. Payroll and recruitment

- There is a risk of recruitment fraud as new staff are needed immediately due to increased demands for services and the normal checks may not be completed.
- Payroll fraud may increase as normal controls around working hours, expenses, overtime etc may be relaxed.
- Staff returning to work to help respond to Covid-19 may be targeted by unscrupulous tax avoidance schemes.
- Telephone calls may be made by fraudsters to health and social care staff requesting personal bank details in order for the £500 'thank you' payment to be made.
- Telephone calls may be received advising staff that their national insurance number has been compromised or is invalid. The caller asks for personal details in order to apply for a new national insurance number.
- Fake Covid-19 related job adverts may appear on social media, eg for Covid testers. The scammers ask for personal details that job applicants typically provide, eg bank details, proof of address and passport details. This information can be used for identity theft.
- Emails may be received purporting to be from HMRC saying the recipient is due a tax refund. The recipient is asked to click on a link to a scam website to provide personal and bank details for the supposed tax refund.

Ways to reduce counter-fraud risks

- Discuss and agree the organisation's risk appetite and associated approach to the newly emerging risks.
- Carry out a risk assessment to identify the most vulnerable areas under the new working conditions. This will include a review of IT system security for remote working.
- Ensure Internal Audit review systems of control. Some of the existing controls are unlikely to be still relevant and appropriate.
- Introduce new systems of control to address new and emerging risks.
- Ensure existing ways of reporting fraud or irregularity are still operating and are promoted, eg fraud hotlines and whistleblowing processes are still operating.
- Review ways of working and delivering services to help ensure those in need are supported.
- Ensure staff and customers receive regular, appropriate communications on the new ways of working and changes to services.
- As staff move back to offices, controls should be reviewed to ensure they are effective and appropriate for the new ways of working. This will include possibly tightening up previously relaxed controls and carrying out audits on assets.
- Consider bank account verification and active company search services, eg that are available to the UK public sector from the Cabinet Office or **NAFN**.
- Continue staff training, especially for staff moved to work in areas that are new to them.
- Continue staff training on counter fraud including new threats. This will include updates on new and emerging frauds as well as reminders that suspicious activity still needs to be reported.
- Run 'dummy phishing' exercises to test employees' reactions, with a requirement to revisit training modules if an employee 'fails'.
- Ensure all software updates are applied as soon as possible to IT systems. This includes regular reviews and updates to all systems and devices and actively looking for vulnerabilities. Where dangerous vulnerabilities are identified, system updates are done immediately even if it means staff can't work while it is being updated. Where a device, eg a laptop, isn't updated, it is disabled and excluded from the network.
- Block and filter every attack vector possible, which can make things difficult for colleagues, and say no to anything that could increase the organisation's susceptibility to attack.

NAFN:

Shared service organisation open to all public-sector organisations. NAFN provides data, intelligence and best practice services for member organisations.

Ways to reduce counter-fraud risks

- Review **NFI** matches to identify fraud and error or system control weaknesses.
- Rotate employees or volunteers working with vulnerable service users and ensure appropriate employee disclosures are up to date.
- Review the NHS Counter Fraud Authority's guidance including the Covid-19 counter fraud guidance
- Review the UK Government Counter Fraud Function's website for the latest guidance including:
  - Covid-19 Counter fraud response team
  - Fraud Control in Emergency Management: Covid-19 UK Government Guidance

NFI:

National Fraud Initiative, an exercise that matches electronic data within and between public and private-sector bodies to prevent and detect fraud.

Further information:

The National Fraud Initiative in Scotland 2018/19

July 2020

A focus on procurement risks

Procurement fraud in the UK is not defined but industry experts put the figure at billions of pounds a year. Procurement fraud is complex and covers a wide range of activities from the pre-contract award phase through to the post-contract phase. Procurement fraud is difficult to detect. Although data analytics to identify fraud are on the increase, manual detection techniques are an important part of fraud prevention approaches.

In order to help reduce some of the risks around procurement, bodies may consider the following:

- All staff should be aware of the potential red flags to look out for within any procurement exercise.
- All staff involved in procurement activity should receive regular appropriate training to help them to identify fraud and error.
- There should be clear processes, procedures and controls to be followed regarding procurement. Checks should be made, eg by internal audit, to ensure these are followed.
- A central contract register should be in place which is regularly reviewed and analysed for irregularities.
- Staff should be extra vigilant where a contract is required in a rush and/or where the contractor may be pressurising staff for a quick response.
- Appropriate controls should be in place to ensure invoices, purchase orders and requisitions all agree before payments are made.
- Appropriate segregation of duties should be in place for the authorisation of contracts, payments and technical specifications.
- Procedures should be in place and followed, for all requests for payments to new bank account details.
- Due diligence should be carried out on new suppliers. This may include a review of online customer reviews, and calling the landline on a website to check it is genuine.
- Consideration should be given to job rotation to ensure staff do not deal with the same clients on a long-term basis.
- Internal audit should review procurement activity, eg through spending analysis, to identify where any large spend to a particular supplier may exceed approval thresholds when aggregated or a review of the security around bids and tender documentation.

Further information:

Red flags

Procurement

October 2019

Fraud and irregularity identified during 2020/21

Auditors have provided Audit Scotland with details of cases of fraud and other irregularity discovered in their audited bodies during 2020/21. This report sets out examples of the various different categories of fraud and irregularity reported during 2020/21 and the control weaknesses which have contributed to these cases.

Reporting cases about fraud and irregularity and sharing information about what happened helps highlight weaknesses in internal controls and aims to help prevent similar circumstances from happening in other public bodies.

Public bodies are encouraged to consider whether the weaknesses in internal control that facilitated each of the cases highlighted in this report may also exist in their own arrangements, and take the required corrective action.

Auditors should confirm that appropriate governance arrangements for the prevention and detection of fraud are in place at their audit clients and that appropriate reviews and amendments of controls have taken place in response to new ways of working. They should also confirm whether internal controls are sufficiently strong to prevent the types of frauds and errors highlighted in this report.

Fraud and irregularity reported during 2020/21 totals £0.4 million

Falls into the following key categories:

2
cyber attacks

5 cases =£132,500
Fraud and irregularity involving expenditure

4 cases = £25,000
Fraud involving payroll

1 case = £237,000
Theft

1 case = £7,000
Involving third party funds

Control weaknesses were highlighted where fraud or irregularity was identified.

Common control weaknesses

A review of fraudulent and irregular activity highlights common control weaknesses which have contributed to the fraudulent and irregular activity reported by external auditors.

- A lack of management checking and review
- Procedures not followed
- Weak security arrangements
- A lack of staff training
- Missing indicators within emails that the email is not genuine
- Not verifying applications for funding to existing records
- Poor budget monitoring
- System reconciliation weaknesses
- Poor record keeping

Cyber attacks

A cyber attack is where computers and networks are targeted by criminals in order to alter, disable, steal or gain information through the unauthorised access to computer systems. Our blog entitled 'Cybercrime is a risk that the public sector in Scotland needs to take seriously,' raises awareness among boards and non-executive directors of this growing area of risk as well as to signpost readers to key resources to help protect organisations from this type of crime.

Case study 1

A public body was subject to a serious complex cyber attack which impacted upon access to systems, processes and communications.

Key features

1.2GB of data amounting to just over 4,000 files had been stolen.

The public body instigated its business continuity plan and took action to limit the impact of the attack. The public body made clear that it would not engage with criminals intent on disrupting public services and extorting public funds.

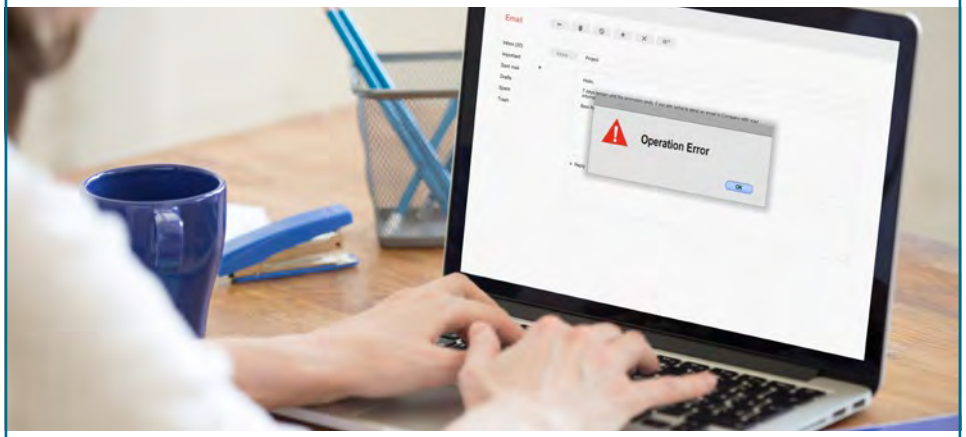
The information that was stolen from the public body's systems was published illegally online on the dark web the following month. The information that was published is still being assessed. IT systems have been disconnected to prevent further data losses.

The impact of this attack will last for some time due to the loss of data, including financial data, and the need to re-build systems and re-create records.

A Police Scotland investigation is under way. The public body is also working with the Scottish Government, the Information Commissioner and the National Cyber Security Centre in order to investigate the specific details of the attack and identify areas to strengthen existing controls.

Case study 2

A cyber-attack caused disruption to services at several colleges.



Key features

The colleges' IT engineers worked to isolate and minimise the impact from the incident.

As a result of the attack, the colleges were closed to some students for a short period of time.

The source of the attack is not known, however a Police Scotland investigation is currently under way.

Expenditure

Expenditure frauds relate to cases where a body has incurred additional expenditure because of fraud. This may be due to invalid suppliers, ficticious invoicing, or the redirection of payments intended for legitimate suppliers.

Case study 3: Invalid supplier

A third party defrauded over £46,000 from a public body by purporting first to be a staff member and then a supplier to the body.

Key features

One of the public body's suppliers received an email purporting to be from the body, asking if there were any outstanding invoices. The supplier replied attaching an invoice. The public body then received an email purporting to be from the supplier with the invoice attached asking for it to be paid to a new bank account. The bank records were amended, and the invoice paid. The fraud was identified when the genuine supplier contacted the body looking for payment of the invoice.

The fraud was possible as:

- the accounts payable department did not confirm that the change of bank details had been verified by the contracting service
- the member of staff within the contracting service had not received training on how to verify new bank details
- indications within the email that it was not genuine were missed
- learning from a previous unsuccessful similar attempted fraud involving the same supplier had not been shared with staff.

The public body is introducing robust verification processes for change of bank details.

Case study 4: Invalid supplier (2)

A third party defrauded £64,500 from a public sector body by purporting to be a genuine supplier.

Key features

The purchase ledger team received several emails purporting to be from a named contact at their utility supply company requesting payment of legitimate outstanding invoices. They included copy invoices from the supplier which appeared to be genuine. The emails requested that the standing bank details be amended to those on the invoices. The bank details were changed, and three payments were made. Remittance advices were sent to the legitimate supplier's email address. The fraud was identified when correspondence was received from the legitimate supplier advising that they had received remittance advice notices but no payment.

The fraud was possible as the procedure for confirming bank account changes was not followed. In addition, the email from the supplier had a subtle difference in the address that was not identified at the time.

All finance staff are now receiving training on fraud prevention and detection. The body has notified Police Scotland.

Expenditure

(continued)

Case study 5: Misuse of a vehicle

A public sector employee defrauded almost £7,000 through unauthorised use of a car over a six-month period.

Key features

The employee was using a hire car while at the same time using a leased car. Both cars were provided by their employer.

The fraud was identified after the payroll team questioned why the car was still on hire.

The fraud was possible due to a lack of review and challenge by the line manager of the monthly car hire report for their department.

The case has been reported to Police Scotland and options for civil recovery are being investigated.

Case study 6: Misuse of vehicle

A public sector employee defrauded over £5,000 over an eight-month period through unauthorised use of a car.

Key features

The employee used a pool car for personal use after their own car broke down.

The fraud was identified after a finance report was issued to the budget holder suggesting that providing the employee with a small van would provide better value for money.

The fraud was possible as the budget holder failed to identify the pool car recharges and investigate accordingly.

Internal audit has reviewed the pool car system to identify system weaknesses.

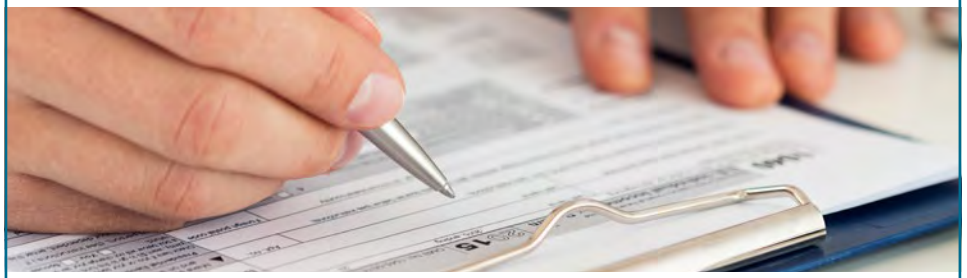
Expenditure

(continued)

Public bodies have been issuing many different grant and funding streams to businesses and individuals over the last year due to the Covid-19 pandemic. There have been many instances of claimant fraud identified in these applications. This report does not include cases of fraud that are perpetrated by claimants, for example, grant claims, unless the fraud was facilitated by either the collusion of local authority staff or by weaknesses in internal control.

Case study 7: Grant payment

A third party defrauded £10,000 from a council by making a false claim for a business grant.



Key features

The perpetrator claimed a business grant for premises they had previously occupied. The fraud was identified when the legitimate business proprietor applied for a grant.

The fraudulent payment was possible as the council failed to identify that:

- the name on the business grant application was not the name of the business on the business rates system
- the bank statement used in support of the application was for a personal bank account rather than a business bank account.

Internal controls have been improved and more stringent checks are now carried out.

Payroll

Payroll frauds relate to cases where an organisation's payroll has been misappropriated, eg employees working elsewhere while claiming to be unfit or where salary payments have been redirected.

Case study 8: Re-directing salary

Four parties defrauded almost £25,000 from four public bodies by redirecting salary payments.

Key features

In all cases, the payroll team received emails purporting to be from genuine members of staff, advising of a change to be made to bank account details. The payroll records were amended, and salary payments were made. The frauds were identified when employees contacted the payroll team to query why they had not been paid.

The fraud was possible as the procedures in place to check the validity of bank detail changes had not been followed.

Payroll staff have been reminded of the proper procedures, including verification procedures for changes to employee bank account details. The cases have been referred to Police Scotland for investigation.

Theft of assets

Theft relates to cases where someone acts dishonestly appropriating property belonging to another with the intention of permanently depriving the other of it.

Case study 9: Theft of assets and cash

An employee misappropriated cash and other assets valued at £237,000 from a public body over a period of eight years.

Key features

The employee was responsible for maintaining records for a secure store. The employee abused their position of trust.

The theft was possible due to inadequacies in the reconciliation of a manual card recording system and in management oversight. The theft was identified when a new process for recording the cash and other assets was introduced and the perpetrator was going to be moved to a new department.

A subsequent internal audit identified the cash and assets were missing. Police Scotland were informed.

The employee admitted the theft, was prosecuted and imprisoned for over three years.

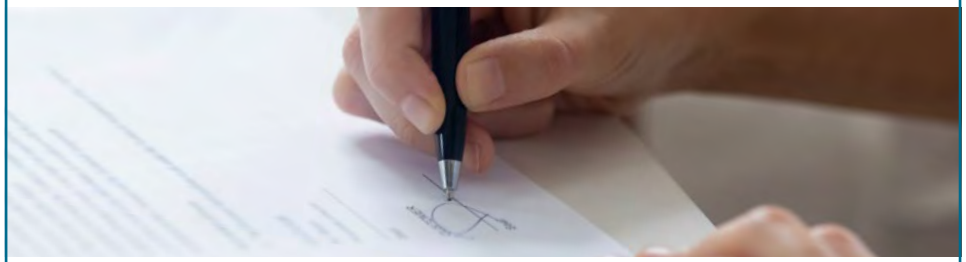
Procedures have been reviewed and improvements made.

Private funds

Private fund frauds relate to cases where third party's funds have been misappropriated.

Case study 10: Third party funds

A member of staff misappropriated over £7,000 from the accounts of vulnerable social care clients.



Key features

The member of staff committed the fraud by forging the signature of another staff member. The fraud was identified when a colleague examined records of client funds and identified an entry that they had apparently authorised but had no knowledge of.

When interviewed, the member of staff admitted forging the signature of a colleague. An internal audit identified the full extent of the fraud.

The fraud was possible due to weakness in record keeping and in the oversight by management and the **Corporate Appointee**. Improvements have been introduced in relation to reconciliation processes and the review of client accounts.

The matter was reported to Police Scotland and disciplinary processes were instigated. The member of staff has repaid the full amount.

Corporate Appointee:

A Corporate Appointee is where an organisation, eg a council, has been appointed by the DWP to manage and look after a customer's welfare benefits to make sure they get the benefits they are entitled to.

Next steps for governance boards in scrutinising counter-fraud arrangements

Strategies

- Are there appropriate and up to date counter-fraud strategies in place?
- Are there appropriate governance and oversight arrangements for the counter-fraud strategies? This will include appropriate performance reporting arrangements.

Risk assessment

- Has an assessment been carried out of where the fraud and error risks lie?
- Has the risk from fraud and error risk been measured and reported? This should be updated regularly.
- Have controls been put in place to prevent and detect these risks?

Controls review

- Are the controls regularly reviewed to ensure they are operating effectively and still appropriate?
- Are controls amended or new controls implemented where new risks emerge?

Further information

You can find further information about Audit Scotland's work to support counter-fraud and good governance on our website. This includes information about:

Website:

Our work on counter-fraud

Report:

Covid-19: Emerging fraud risks

July 2020

Report:

Red flags in procurement

October 2019

Website:

The National Fraud Initiative

Report:

How councils can safeguard public money

April 2019

Blog:

Cybercrime: A serious risk to Scotland's public sector

May 2021

Fraud and irregularity 2020/21

Audit Scotland's published material is available for download on the website in a number of formats.
For information on our accessibility principles, please visit:
www.audit-scotland.gov.uk/accessibility

AUDIT SCOTLAND

Audit Scotland, 4th Floor, 102 West Port, Edinburgh EH3 9DN
T: 0131 625 1500 E: **info@audit-scotland.gov.uk**
www.audit-scotland.gov.uk

ISBN 978 1 913287 55 9

Find out more
www.thebci.org

bci Thought Leadership

BCI Horizon Scan Report 2022

bsi.

bci Leading the way to resilience

Contents

5 Executive summary

10 Risk and threat assessment: past twelve months

22 Risk and threat assessment: next twelve months

30 Consequences of disruption

35 Benchmarking business continuity

44 Benchmarking longer term trend analysis

56 Annex

Foreword

I am pleased to introduce the 2022 BCI Horizon Scan report, one of the most established annual reports in our portfolio. We are very grateful for the continuing support of BSI, our longstanding partner in the production of this report.

This year's report falls at a critical point. Organizations are, in many countries, starting to return to a degree of normality after COVID-19 severely disrupted operations for two years. However, with the waning of COVID-19, the world is now faced with the Ukraine crisis.

We noted in our 2020 report how organizations were sorely unprepared for COVID-19. The statistics showed that non-occupational disease — which includes pandemic — was at the second bottom of the list in terms of concerns for 2020. The survey closed at the end of December 2019. Meanwhile, this year's report shows that Business Continuity, Resilience and Risk professionals' thoughts remain dominated by the pandemic, with incidents such as exchange rate volatility, political change, violence and civil unrest and natural resources shortages ranking towards the bottom of the table for concerns for 2022. The survey for this year's report closed just before news of the escalating situation in the Ukraine was first discussed in the media.

Organizations have made significant learnings from the pandemic — business continuity and resilience staff have been propelled to the forefront of many organizations by senior management. This has resulted in practitioners' roles becoming more strategic with leadership and boards asking for guidance about how new strategies will work from a business continuity and resilience perspective. Funding has increased, staffing levels have risen and there is an increased demand for training and exercising. There has also been an eleven percentage point increase in the number of organizations who are now using the ISO 22301 standard as a framework.

However, while our industry has made significant progress since the start of the pandemic, horizon scanning and risk mapping still needs improvement for many organizations. The most astute professionals had seen issues developing in Ukraine weeks before the mainstream news broke out and spent time firming up cyber security and reviewing supply chains.

The primary learning from this report is that we still need to be prepared for the unexpected. While we have seen many members breathe new life into their programs and our industry over the past two years, there is still work to be done in terms of risk planning and ensuring organizations are prepared for anything — however unlikely it may appear at the time.

I would like to thank our members and contacts once again for their valuable insight in making this report possible. We have once again been inspired by some of the stories we have heard in our interviews and would like to thank practitioners for being at the forefront of ensuring their organizations and industries are truly resilient. I would, once again, like to offer my sincere appreciation to the BSI for the continued and valued support of this report.

Christopher Horne FBCI
Chair of the BCI

bsi.

Foreword

The latest BCI Horizon Scan Report 2022 reveals the key issues that have dominated organizations' risk landscapes over the last year and the ones expected to dominate in the coming years.

Organizational Resilience is an overarching topic on which BSI has been working for many years, and we are pleased to continue the collaboration with the BCI on how business continuity expertise and best practices contribute to resilience.

The latest insights shed light on the ongoing and emerging global risks and threats for organizations, their people, their data, and their extended value chains and ecosystems.

This year's report recognises the inter-connected world we live in as business continuity has been challenged yet again in the face of economic uncertainty. It has proven once again increasing relevance in helping organizations better prepare to face the climate crisis, changing working practices and other major disruptions.

The report makes clear the threat of the pandemic still lingers in 2022, with non-occupational disease becoming the primary perceived risk to organizations and their staff.

Hybrid workplace environments are increasingly testing organizations and bringing additional risks — from health and safety concerns to wellbeing issues to ensuring homeworkers' remote environments are as resilient as those in the office — meaning cyberattacks and data breaches will be critical considerations for organizations for years to come.

The findings show that the consequences of any disruption are not just organizational but predominantly human, particularly on staff morale and wellbeing. That is why those companies that focus on their people will in turn increase their potential agility and ultimately their resilience.

It is encouraging to see the progress achieved in using best practice standards, not only the international standard on Business Continuity Management Systems (ISO22301) but also other good practices that contribute to the resilience of companies, large and small.

Organizations that continue to embed best practice to increase the agility of their teams will be better prepared to adapt to new, emerging global risks as well as to unpredicted and somewhat unpredictable events.

This report, even more than previous editions, confirms that leaders who continue to focus on enhancing the resilience of their organizations in the constantly changing and turbulent business environment will become more trusted, more resilient and, ultimately, future-ready.

Pietro Foschi
Group Executive Director Assurance Services
BSI

Horizon Scan 2022
Executive summary

Executive summary

Preparing for the unexpected: The 2020 and 2021 editions of Horizon Scan showed that many organizations were not prepared for the disruption caused by COVID-19. Plans had to be rewritten from scratch, technology hardware had to be sourced through disrupted supply chains and workplace environments had to be altered to ensure staff could work remotely and, for those that could not, strict social distancing policies had to be adhered to. Organizations spoke about how they will now be considering risk on a much broader scale, so similar 'surprises' could be mitigated for the future. Whilst progress has been made, the crisis in the Ukraine has also caught many organizations by surprise. Respondents spoke how they would now change their answers to the survey, ranking risks such as 'political conflict' higher, had they known about the Ukraine crisis earlier. Preparing for the unexpected is a primary theme for this year's report.

Hybrid workplace environments are testing organizations: Organizations are now 'normalising' their working environments now COVID is proving less of a threat to life and staff are able to return to offices. For many organizations, this means continued remote working or working in hybrid environments which both come with risks: from health and safety concerns and mental health issues to ensuring homeworkers' remote environments are as resilient as those they would expect in the office.

Non occupational disease remains the primary perceived threat to organizations and their staff: Risks belonging to natural domain, ranging from the possibility of new viruses to extreme weather events, are something practitioners need to address regardless of industry, country, and size. In this regard, respondents state that climate change will be one of the greatest threats in the next five years.

Cyber threats increased during the pandemic – and are now on a steep rise again: Cyber security is the second-ranked concern for the following year after non-occupational disease. Cyber-security concerns increased during the pandemic with criminals exploiting homeworkers through social engineering and targeting hastily constructed networks that lacked security. The crisis in the Ukraine has caused a four-digit percentage point rise in cyber-crime since the invasion began, with attacks causing more devastation for some organizations than ever noted previously.

Supply chain disruptions are also on the rise, as the global shortage for several types of products and services continues: Supply chain threats can arise from several types of challenges, whether these are human resource management, biological and environmental risks, civil unrest or cyber resilience issues. Indeed, as recently as 1 March, Toyota announced that it was halting production due to a cyber-attack on one of its critical suppliers.

Management are better understanding the importance of resilience and business continuity management in their organizations: Respondents reported better management of disruptions in the past year thanks to international best practices. Indeed, Management were driving greater adherence to international standards (such as the ISO 22301 standard) leading to improved relationships between resilience-orientated departments. It is time for the several management disciplines to come together and work with units that so far have not been included enough in the resilience discourse, such as change management.

Risk and threat assessment

Past twelve months

Non-occupational disease has continued to dominate agendas during 2021

Non-occupational disease:
24.5

Remote work:
24.3

Travel restrictions:
21.5

Health incident:
17.9

Lack of talent:
17.3

Next twelve months

Are we prepared for the unexpected? Non-occupational disease is still considered the primary risk for 2022

Non-occupational disease:
7.8

Cyber attack & data breach:
6.9

Travel restrictions:
5.6

Remote work:
5.0

IT and telecom outage:
4.9

Consequences of disruption

The human consequence of disruption is having the most impact on organizations

Negative impact on staff morale/wellbeing/ mental health:
68.1%

Loss of productivity:
62.1%

Staff loss or displacement:
44.3%

Loss of revenue:
42.0%

Supply chain disruption:
41.3%

ISO 22301 update

Certifications were down slightly in 2021, but uptake of the standard as guidance has increased by eleven percentage points

We use ISO 22301 as a framework but are not certified to it:
56.0%

We use ISO 22301 as a framework, are not certified to it, but are in the process of getting certified:
5.3%

We use ISO 22301 as a framework and certify to it:
9.8%

We don't currently use ISO 22301 as a framework but we intend to move towards this during 2022:
7.6%

We don't use ISO 22301 as a framework and have no plans to move towards this during 2022:
21.3%

Benefits of certification

The external benefits of certification and exhibiting to stakeholders the effectiveness of BCM programmes are the prime certification benefits for organizations

Allows us to demonstrate the effectiveness of our BCM programme to external stakeholders:
74.0%

Increases our organization's resilience:
74.0%

Enables the management of disruption:
60.0%

Enables consistent BCM measurement and monitoring:
60.0%

Enables faster recovery after a disruption:
54.0%

Benchmarking longer-term trend analysis

Most organizations carry out risk and threat assessments to perform trend analysis, but use of other sources is sporadic in some organizations

Internal risk and threat assessment:
88.2%

External reports/ industry insight:
77.3%

Risk registers:
71.4%

Participation to industry events/conferences:
62.3%

Social media monitoring:
39.6%

Investment in business continuity

Just 8% of organizations expect invest in business continuity to be cut in 2022

Investment levels will be increased:
33.9%

Investment levels will be maintained:
46.6%

Investment levels will be decreased:
8.1%

Overview

Last year's Horizon Scan Report captured a risk landscape that remained dominated by COVID-19 and told how the virus had caught most practitioners unaware. The 2020 report — published at the beginning of the pandemic — had non-occupational disease featuring second from bottom as a future risk. The survey for the 2020 report closed just a day before the news of COVID-19 first broke out.

The 2021 report served as a lesson in being prepared for the unexpected. Respondents explained how the experience of COVID-19 had encouraged their organization to take a broader view of risk and consider more of those risks which had previously been deemed unlikely to happen. This year's report shows a similar picture to the 2020 Horizon Scan. Respondents filled in the survey in December and early January, and still placed non-occupational disease as their top threat for 2022. However, when speaking to some of the respondents, many told how they would now change their answers given the escalating situation in Ukraine.

The Ukraine conflict is affecting global supply chains and setting financial markets into shock. According to a large managed services provider in the United States, cyber-attacks have increased by 800%[1], causing major damages to organizations' operations.[2].

That said, being aware of wider risks is a theme which came from both the survey and interviewees, and the attention of management towards the risk and the business continuity processes around this remains heightened. A greater appreciation of resilience is now widespread amongst organizations: 22.2% of interviewees reported their organizations had created the role of Chief Resilience Officer at board-level in the past year.

Some of this heightened awareness by management is also being seen in the uptake of standards. We have noted an 11-percentage point increase in the number of organizations who are choosing to align to ISO 22301 standard. Moreover, whilst there has been a slight dip in certifications this year, many practitioners report that certification is now a possibility for their organization for the first time.

Once again, this report continues to be a lesson on preparing for the unexpected, as well as for incidents that can arise from a crisis such as COVID-19 and the escalating situation in Ukraine.

1. Burt, J. (2022). Dunno about you, but we're seeing an 800% increase in cyberattacks, says one MSP. The Register [online]. 11 March 2022. Available at : https://www.theregister.com/2022/03/11/russia-invasion-cyber-war-rages/ [accessed 15 March 2022]
2. Tidy, J. (2022). Ukraine crisis: 'Wiper' discovered in latest cyber-attacks. BBC News [online]. 24 February 2022. Available at: https://www.bbc.co.uk/news/technology-60500618 [accessed 15 March 2022]

Risk and threat assessment: past twelve months

Risk and threat assessment: past twelve months

- **The pandemic continued to dominate organizations' agendas in 2021.**
- **Supply chain concerns continued into 2021. The Suez Canal incident had a major impact, but global shortages of certain goods (such as microchips) remain endemic.**
- **Organizations are working hard to ensure they have failsafe cyber-security measures, but staying one-step ahead of attackers remains challenging, particularly with the ever-increasing number of attacks.**

For the second year running, the pandemic makes the top of the risk score index, with non-occupational disease (24.5) being the most impactful event of the last 12 months. However, whilst the risk score is significantly higher than that noted in 2020 (18.6), this is down to the frequency of events related to the pandemic. The impact score decreased year-on-year to 2.5 out of a possible 4 (2021: 3.2) as organizations started to understand COVID-19 better and adapted their processes and procedures accordingly. Indeed, interviewees described how COVID-19 had been increasingly considered business-as-usual (BAU) during 2021.

However, whilst organizations are getting better at managing the threat posed by COVID-19, the first four ranked incidents are directly related to the pandemic and its resultant effects on organizations. The responses demonstrated how COVID-19 caused a long series of knock-on effects in various areas, ranging from the transformation of business processes to the deterioration of mental health for personnel.

In this year's index, issues arising from remote work, or a new workplace environment were in second place with a score marginally lower than non-occupational disease (24.3). The shift to a different office paradigm is something which few organizations would have envisaged 24 months ago. As organizations around the world adapted to a significantly different way of working, employers had to ensure their workforce had the right equipment (e.g., laptops, stable connections) and that the office IT infrastructure was suitable enough to stand the test of physical restrictions. From a business continuity (BC) perspective, plans had to be rewritten to ensure workers had the same BC backup that they would if they were working in the office. Although many respondents admitted that there was still work to be done to ensure remote workers were covered from a BC perspective, some organizations have this firmly integrated within their plans. One interviewee highlighted that they had gone so far as to request remote senior management staff purchase generators. Another said they ensured they had dual backup when operating in a remote environment.

"I meet with the department heads and senior management regularly and we discuss remote risks, what the impacts could be and how to mitigate those risks. Not only are we continually looking at them, but senior management is also continuously looking at it and keeping it in mind when trying to decide whether or not to keep certain people remote in certain locations. So, for example, when hurricane season is approaching we need to decide whether to bring workers into the office, make them remote, or ask them to work in another location. We are just trying to keep our options open. One of the things we have also done is asking some of the executive remote staff if they could purchase power generators. This decision was made after learnings from the Texas freeze last year. We had executive management that were unable to work for two weeks because cars were in the garage and the garage froze shut. Thus they were unable to use their car as a power source for their laptops. And they obviously couldn't go into the garage to start the car without the risk of carbon monoxide poisoning."

Senior Business Resiliency Manager,
Healthcare, United States

"For some critical roles which became remote, we had to give them dual links; dual service providers. This ensured that if one service process went down, we could give them an alternative by switching them across immediately. That's what we did for the critical teams that were managing those areas, and teams that are time bound by processes."

Head of Continuity Management,
Financial Services, Zambia

Our interviewee from Zambia - where internet banking is not widespread - explained that remote working has been an issue as most customers still want a 'bricks and mortar' bank. However, the particular practitioner used his experiences with a previous employer to ensure his current organization could run as effectively.

"My previous employer was [another major bank] where we had already established structures around remote working. So when I came here, I quickly set up the remote working and ensured testing took place. So when you do the testing many won't agree to it, but it's something that I have now had to start initiating as a way of testing the business continuity plans. There was a lot of pushback; they didn't realize what was coming up until COVID-19 hit the country. That's when everybody appreciated the testing that had gone on. Then we had to put in a hybrid working and put about 80% staff work remotely. For our branch network, we got branches to start rotating opening days and times. This impacted on our customer service as many people in Zambia still believe in brick and mortar queues and carrying out processes within a branch. Whilst there were lots of queues, we have now started delivering on the digital products."

Head of Continuity Management,
Financial Services, Zambia

In last year's Horizon Scan Report[3], Members also discussed the problem of 'double whammy' events. This was a particular concern for organizations in areas prone to extreme weather, where BC professionals were not only having to ensure continuity of operations during the pandemic, but also sometimes during 'double whammy' scenarios (such as bushfires and concurrent flooding). Many have learned from this and, as a result, are more prepared for future events.

One interviewee mentioned how they had had to alter their whole operating model to be able to cope with the changing consumer environment during the pandemic. This obviously required additional resource from business continuity.

In the near future, remote work is set to become a must-have for most organizations[4]. Furthermore, today's workforce is more aware of their right to choose an employer as much as an employer chooses them. Thus, a well-developed remote work policy has the potential to become a competitive advantage in attracting and retaining talent. Another effect of such change could lead organizations to move away from the mere quantification of work and pay greater attention to outcomes. In addition, remote work appears more environmentally friendly and socially responsible for a variety of reasons, such as fewer commutes and better management of stress levels.

Such changes lead to another risk for organizations that of talent attrition. This is why, in 2022, it is not surprising to see this lack of talent/key skills in fifth position, with a score of 17.3 (2021: seventh position; 12.1). One interviewee, based in Australia, commented that the lack of available IT personnel was creating a threat to the resilience of IT and telecommunications systems within their educational establishment. Another interviewee from a larger corporation also spoke about the lack of available IT and technical staff.

"One thing that is really prominent is the dependency on IT and telecom management and the consideration that there's not been any testing of our backup. So over the last two years I've been working with a number of IT managers, because of staff turnover, to understand this. Also, now schools are using technology to deliver education there has been little consideration for what would happen if it didn't work the way they thought it would. As a result, we're doing some scenario analysis across the school about what would happen if we actually lost communications for a day, a week, year? And the reliance on physical servers for so much raises additional questions."

Risk & Compliance Officer, Education, Australia

3. Elliott, R: BCI Horizon Scan 2021. The BCI. March 2021. Available at: https://www.thebci.org/resource/bci-horizon-scan-report-2021.html [accessed 15 March 2022]
4. Granieri, A (2020). How the Remote Work Revolution Will Change the Employer/Employee Relationship. Gartner.com. July 2020. Available at: https://www.gartner.com/en/human-resources/trends/remote-work-revolution [accessed 15 March 2022]

The same interviewee also commented how the pandemic had changed employees' working preferences. Many had become demoralised with the teaching environment, or with the possibilities of remote working, and wanted to work in a role which did not require a lengthy commute.

> **"Through the pandemic, the loss of staff experienced presents a loss of good talent and difficulty in finding suitable replacements. It's driven predominantly by people who just don't want to do this kind of work anymore or don't want to commute. Having to teach within an online environment didn't suit a lot of people in the industry. Initially I was concerned, but found it's widespread across Australia and some parts of the world. So that made me feel better. But it doesn't negate the issue that we have. I just don't have confidence in the IT process in itself."**
>
> Risk & Compliance Officer, Education, Australia

> **"The shortfall in availability of talent with key skills is a risk which has been openly acknowledged across the organization, such as IT engineers and cybersecurity specialists. COVID resulted in our migrant stream being stopped in Australia, which has always been a very strong source of talent for those sorts of skills for all organisations. Therefore, this is one that the organisation is looking at very hard as we build and improve our technology stack and the resilience."**
>
> Group Business Resilience Manager, Financial Services, Australia

Travel restrictions — another direct consequence of the pandemic — ranks third in the risk table, with a score of 21.5. Hindrances to free movement, both locally and internationally, have been at the top of the agenda in recent times, with different countries adopting different policies, which have generated confusion and mental fatigue for citizens. It is also worth noting that such policies have often changed due to updates in the rates of infection and vaccination. In this regard, the uneven access to vaccines has led to a significant advantage for some countries who were able to acquire vaccines easily, whereas some were — and still — have not received enough. This means that trade is highly facilitated for richer countries, who can reopen and restart production earlier than those left behind. The world average of individuals having completed the vaccination cycle stands at 62%, and while countries in Europe and North America are well above those levels, several developing countries have yet to reach 10%[5].

Health incidents (non-COVID related) are in fourth place in this year's risk index. The category, which includes occupational disease and mental health, was second in last year's report and, if it were not for the two new incident categories of remote working and travel restrictions being added in this year's report, it would most likely be in second place again.

UK statistics reports on health and safety are a good example of how worrying and complex the situation is. Without considering the direct impacts of COVID-19, 1.7 million workers in the UK suffer from work-related illness, with roughly 800,000 of them dealing with stress, depression, and anxiety, and an additional 500,000 battling musculoskeletal disorders. Furthermore, incidents in the workplace still affect nearly half a million individuals every year[6]. Although the overall risk index score fell marginally this year to 17.9 (2021: 18.2), the frequency score for health incidents is higher this year (9.4) than last year (7.8). It appears that whilst organizations may be getting better at offering support to staff who may be experiencing difficulties, the frequency of such issues shows no signs of abating.

As discussed above, lack of talent and key skills (17.3) rounds up the top five, confirming that today's organizations need to do more than simply advertise a vacancy to get the right candidate for the job.

5. Our World in Data (2022): Coronavirus (COVID-19) Vaccinations. OWID. Available at: https://ourworldindata.org/covid-vaccinations [accessed 15 March 2022]
6. UK Health & Safety Executive (2021): Health and Safety at work. HSE/National Statistics. Available at: https://www.hse.gov.uk/statistics/overall/hssh2021.pdf [accessed 15 March 2022]

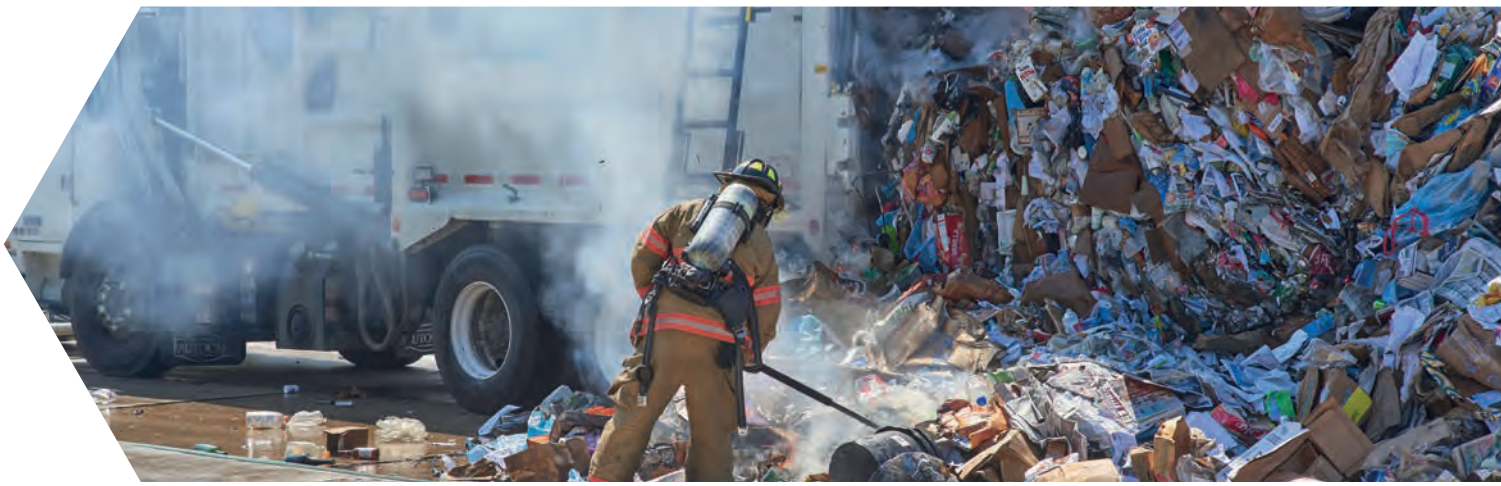
Workers are now more demanding with their requirements for jobs (e.g. requiring full-time remote working, extra benefits), others have left their sectors entirely or, in the case of some, left for other countries because government rule changes stopped them working because of escalating violence, or because they could work for other organizations remotely from abroad.

In the past year, increasing numbers of workers have been leaving their jobs mainly due to working conditions and job satisfaction — so much so that this phenomenon has been nicknamed the 'Great Resignation'[7]. 2020 proved to be a wake-up call for many employers to reassess their priorities and focus on their employees' physical and mental health. Indeed, the way employers behaved through the pandemic showed a tangible link to their ability to retain employees. This, much like remote work, is a challenge that is here to stay; thus, employers should ensure they remain ahead of their peers in terms of employee support and remuneration or they may hit problems with talent retention and acquisition. As a valuable addition to their analyses, organizations should run competitive intelligence programmes and map out competitors' staff packages.

On a similar note, physical safety incidents (14.5) are another prominent issue which relates to workforce retention. In last year's report, this category saw an increased risk score of 16.1; which was blamed in part to staff absences which required unqualified staff to operate machinery, and incidents in remote working environments which had not been subject to risk assessments. This year, thankfully, the lowered score suggests that organizations are now taking more consideration of unsafe working environments, and we are anecdotally hearing that more organizations are undertaking video risk assessments of remote working environments.

However, a recent report by EcoOnline, the Hybrid Working Survey[8], showed that less than half of organizations (47%) have provided training for staff in issues such as home office ergonomics, remote communications or techniques for isolation. Moreover, a third of organizations (32%) have failed to carry out risk assessments for workers' remote environments. As organizations' post-pandemic working models are beginning to be set in stone, and remote/hybrid environments are becoming the norm in many sectors, ensuring that basic risk assessments are carried out on workers' remote setups should be at the top of the list for HR and/or operations management.

An interviewee highlighted how meeting the challenges of operating within different regions in the UK during COVID was difficult as each region had different rules to adhere to which created safety concerns. The same interviewee also added that changing working conditions during the pandemic had resulted in an increase in fires at waste depots as the increased population working from home meant an increase in the number of batteries being incorrectly disposed of. This demonstrates that resilience professionals should not just think about the direct implications on business continuity in the event of a pandemic but consider the wider context of how knock-on effects in changing consumer behaviours will impact the business.



7. Morgan, K (2021). The Great Resignation: How employers drove workers to quit. The BBC [online]. 1 July 2021. Available at https://www.bbc.com/worklife/article/20210629-the-great-resignation-how-employers-drove-workers-to-quit [accessed 15 March 2022]
8. WcoOnline (2021): How have we managed the risks of Hybrid Working? EcoOnline. Available at: https://www.ecoonline.com/how-have-we-managed-the-risks-of-hybrid-working-survey (accessed 15 March 2022)

Supply chain disruption (13.3) ranks seventh in the risk score index (2021: 12.0). It is not surprising that supply chain made it to the top ten again — and with a higher risk score — given the ongoing global supply chain and logistics crisis. As economies struggled, the demand for essential goods increased dramatically, placing an ever-greater pressure on suppliers to deliver, particularly against a backdrop of increasing consumer propensity for online ordering adding additional workload to light haulage. Adding fuel to the fire, the Suez Canal incident led to more delays and backlogs[9]. This, coupled with a general lack of focus on supply chain resilience, created the perfect storm for the global logistics industry to enter into a crisis that seems to be still far from over. Unfortunately, building response and recovery capabilities within supplier networks has not received enough attention by organizations worldwide. As reported in the *BCI's 2021 Supply Chain Resilience Report*[10], most companies (80%) have BC arrangements in their supply chain, but only about half of them seek some sort of verification such as evidence of exercises or proof of certification.

> **"We saw a big disruption to supply of IT equipment in 2021 because of the worldwide post-Covid chip shortage and the Suez Canal blockage, 6 days in March 2021. Anything with a chip, not just computers, but lots of electronic equipment. That was a once-in-a lifetime occurrence. The impact was completely unexpected because nobody realized how much stuff was coming through the Suez Canal to Ireland."**
>
> Business Continuity Professional, Higher Education, Ireland

Moving away from physical threats, eighth and ninth place in the risk score features IT and telecom outage (12.3) and cyber-attacks and data breach (11.7) respectively. While compared to last year, these two risks are down from fifth to sixth place, they still represent a significant challenge for organizations.

Cyber resilience should be a critical asset for modern organizations, and it is a key capability due to the growing digitization of business processes, remote work, and uptake of e-commerce. As the world relies more and more on hybrid workplace environments, it is essential that IT infrastructures are reliable and secure. In the last two years, cyber-attacks have not only increased, but they have also been tailored to current events. Phishing emails with links to fake healthcare portals, targeted attacks to hospitals, and charity donations scams are now among the preferred attack vectors in the online criminal underworld. The larger adoption of virtual processes has broadened the attack surface for perpetrators that can take advantage of weaknesses such as more access points, low computer literacy, and inability to distinguish reliable sources on the internet.

However, with cyber-attack and data breach nearing the top of the table for future risks in 2022, these particular incidents are top of mind for senior management and BC professionals. Furthermore, with global tensions increasing as a result of the Ukraine crisis, cyber security is likely to receive even more attention in organizations' plans.

9. Grynspan, R (2022). Here's how we can resolve the global supply chain crisis. World Economic Forum [online]. 17 January 2022. Available at: https://www.weforum.org/agenda/2022/01/resolve-supply-chains-crisis/ (accessed 15 March 2022)
10. Elliott, R (2021). BCI Supply Chain Resilience Report 2021. The BCI. Available at: https://www.thebci.org/resource/bci-supply-chain-resilience-report-2021.html (accessed 15 March 2022)

"The Board are very concerned about cyber security. Whenever there are any cyber events on the news, they always ask our CIO and CISO that preparedness question, 'What does this particular event mean for us? Could we be susceptible?'. And so that thirst for reporting is ever present. We used to do a quarterly board update, and that's been moved to monthly board updates just in the last few months as well. The pressure from above to demonstrate preparedness is 100% there."

Resilience Professional, Utilities, United Kingdom

"We have several staff who are joint appointments between the University and the Health Service Executive [HSE]. This also applies to other universities in Ireland that offer medical programs. When the HSE system was closed down, this caused knock-on effects with our linked machines too. It was a huge unintended consequence, because the attackers were aiming at the health system, but they got at the university system as well through the links between the university system and the health system."

Business Continuity Professional,
Higher Education, Ireland

An interviewee from the university environment explained how they were particularly vulnerable to cyber-attacks due to links with the health service authority - an external network. This demonstrates that professionals should ensure not only their systems are secure, but also that their linked systems have BC back-up in the event of a cyber-attack. On 14 May 2021, the Irish Health Service Executive (HSE) suffered a major ransomware cyber-attack which caused all of its IT systems nationwide to be shut down. It was the most significant cybercrime attack on an Irish state agency and the largest known attack against a health service computer system.

Rounding up the top ten, lone attacker and active shooter incident scored 11.1, rising from number 21 in the 2021 report. As highlighted in the 2021 Horizon Scan report, it is important that organizations do not disregard a certain risk only because it is not in the top half of the chart. It is always necessary to evaluate critical assets and understand whether they might be vulnerable to a specific event, as every process or service has its own specificities. For instance, facilities might be subject to physical violence, which registers the highest impact score after non-occupational disease. Such incidents also show how different environments can change the risk profile for a specific incident. In 2020, while many organizations were operating partially or entirely remotely, the risk from lone shooters was lessened. Now that organizations are returning to more office-based environments, the risk of onsite incidents (such as lone attackers) is likely to increase as a result.

Another important theme to follow is that of weather events, as the effects of climate change are becoming very visible. Therefore, strategic and operational activity to mitigate against climate risk is required now more than ever, both from a BC and regulatory perspective. The index includes several climate-related risks such as extreme weather (10.9) in 11th position, natural resources shortage (10.3) in 13th position, and natural disasters (7.9) in 22nd position. Although all these are outside the top 10, with increasing attention on climate risk on global corporation agendas, they are now being considered more readily within organizational risk registers — even for regions which were not traditionally associated with climate-related disruption.

Among the trends to watch, it will be important to pay attention to political violence (19th position with a score of 9.4) and energy price shock (18th position with a score of 9.2) as global tensions are on the rise due to the situation in Ukraine and other areas of conflict. Also, regulatory changes, 12th with a score of 10.9, might put pressure on organizations to implement better resilience measures, as in the case of the Operational Resilience directives issued by the Bank of England.

Rank	Event	Frequency	Impact	Risk Index
1	Non-occupational disease (e.g. pandemic)	9.7	2.5	24.5
2	(Issues arising from) remote working/new workplace environment	11.4	2.1	24.3
3	Travel restrictions	10.0	2.1	21.5
4	Health incident (NOT transmissible disease such as COVID but occupational disease, reportable occupational disease, stress/mental health, increased sickness absence)	9.4	1.9	17.9
5	Lack of talent/key skills	8.0	2.2	17.3
6	Safety incident (personal injury, fatality, asset damage, dangerous occurrence, reportable incident)	7.8	1.9	14.5
7	Supply chain disruption	6.3	2.1	13.3
8	IT and telecom outage	6.1	2.0	12.3
9	Cyber attack & data breach	6.0	2.0	11.7
10	Lone attacker/active shooter incident	4.8	2.3	11.1
11	Extreme weather events (e.g. floods, storms, freeze, etc.)	5.4	2.0	10.9
12	Regulatory changes	5.2	2.1	10.9
13	Natural resources shortage	5.2	2.0	10.3
14	Higher cost of borrowing	5.4	1.9	10.2
15	Interruption to utility supply	5.0	1.9	9.7
16	Exchange rate volatility	4.8	2.0	9.6
17	Political violence/civil unrest	4.9	1.9	9.4
18	Energy price shock	4.5	2.0	9.2
19	Political change	4.0	2.2	8.6
20	Introduction of new technology (IoT, AI, Big data)	4.4	1.9	8.4
21	Critical infrastructure failure	3.9	2.1	8.2
22	Natural disasters (earthquakes, tsunamis, etc.)	4.3	1.9	7.9
23	Enforcement by regulator	3.7	2.0	7.2
24	Product safety recall	3.2	1.8	5.6

Table 1. Please insert the frequency that events have occurred and the associated impact levels on your organization from the list of events below:

Risk and threat assessment: past twelve months

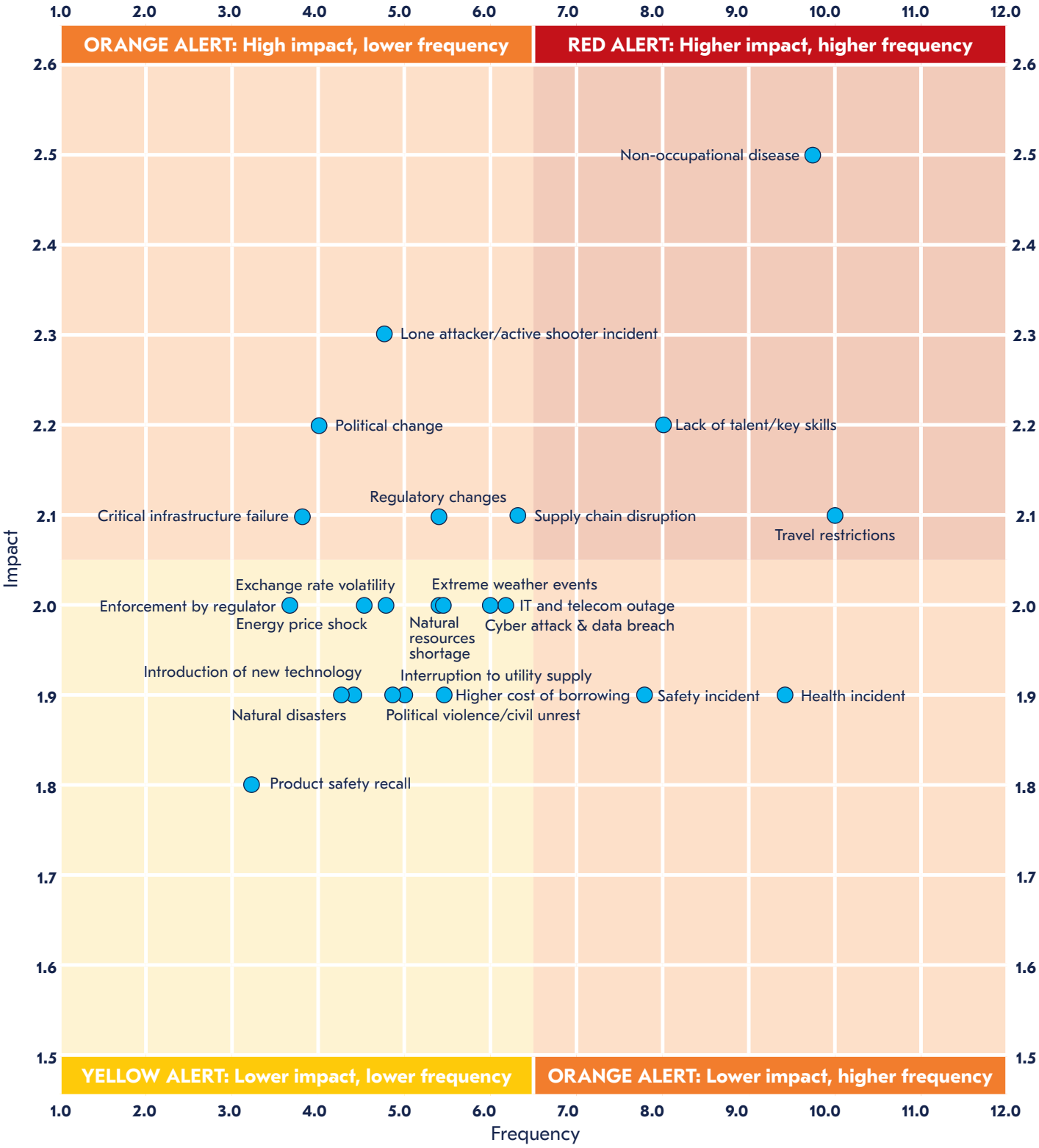


Figure 1. Risk and Threat Assessment: Past 12 Months

In addition to labeling the frequency and impact of all incidents over the past year, respondents were also asked what the cause for their largest disruption of 2021 was. It is of no surprise that the greatest disruption in the last twelve months was caused by non-occupational disease (35.8%), but it is interesting to observe that for 12.6% of the respondents, IT and telecom outage represented the most relevant event. As highlighted in the risk score analysis, the long-term switch to homeworking requires resilient IT networks and doing so on a permanent basis can be challenging. We are also seeing many organizations become increasingly reliant on one particular platform for all their IT and communications solutions. Whilst using a company such as Microsoft for all processes might be a satisfactory solution, from an operations perspective it does come with risks. A global Microsoft outage in April last year meant users were unable to access numerous Microsoft services, including Microsoft Office, Dynamics 365, Teams, OneDrive and Yammer[11].

The *BCI Emergency Communications Report 2022* also showed how many organizations were now routing all voice calls through voice-over-IP (VoIP) — and some even routing through Teams. If a backup solution is not in place, an organization risks losing all access to voice calls. Some organizations are now reverting to having PSTN backups to VoIP solutions but even some of those need careful consideration: in the UK, for example, the PSTN network is being grandfathered in 2025.

Supply chain disruptions (7.1%) were also problematic for organizations in 2021 and the lasting shortage of key components across different sectors is now starting to feel more of an endemic issue rather than a one-off incident. Furthermore, with newer complications entering the landscape, such as the conflict in Ukraine, supply chains are facing even greater challenges in the new future.

Completing the top five, extreme weather events (6.3%), remote work (5.9%), and travel restrictions (5.5%) were all equally significant in disrupting operations - revealing once more how complex and varied the threat landscape has become. In some parts of the world, extreme weather has caused more of an impact than the pandemic. For example, Madrid (Spain) witnessed its heaviest snowfall in 50 years; Fiji experienced category 5 cyclones; in the US, Texas saw heavy winter storms which resulted in 3.5 million businesses and homes left without power, and Oregon saw its largest bushfires in history.

New South Wales (Australia) suffered extreme flooding and in Europe, Germany was hit by heavy floods and Greece experienced extreme heat which sparked wildfires forcing evacuation of the country's island, Crete.

In isolation, these events could be considered as one-off events which can be treated as acute incidents and BC works to get essential services back up and running as soon as possible. However, some organizations are now admitting that climate risk is being seen as more of a 'chronic' risk and they are seeking to try and mitigate against more severe weather going forward (e.g. moving entire operations from at risk areas, providing staff with power backup if they cannot attend their place of work or choosing suppliers who are not located in at risk regions).

"We have invested a significant amount on flood defences in the last decade. Some substations and compressor stations are on flood plains but they've all been strengthened — literally raised up in places — and defences put in place for them. Climate change impacts on our resiliency is a definite concern with the rising temperatures. The more extremes that are becoming apparent, the more our resilience will be tested. We are making efforts to strengthen our whole network."

Resilience Professional, Utilities, United Kingdom

11. Abrams, L (2021). Microsoft outage caused by overloaded Azure DNS servers. BleepingComputer [Online]. 3 April 2021. Available at: https://www.bleepingcomputer.com/news/microsoft/microsoft-outage-caused-by-overloaded-azure-dns-servers/ (accessed 15 March 2022)

Please indicate below which of the above event was your most major disruption in the past year:

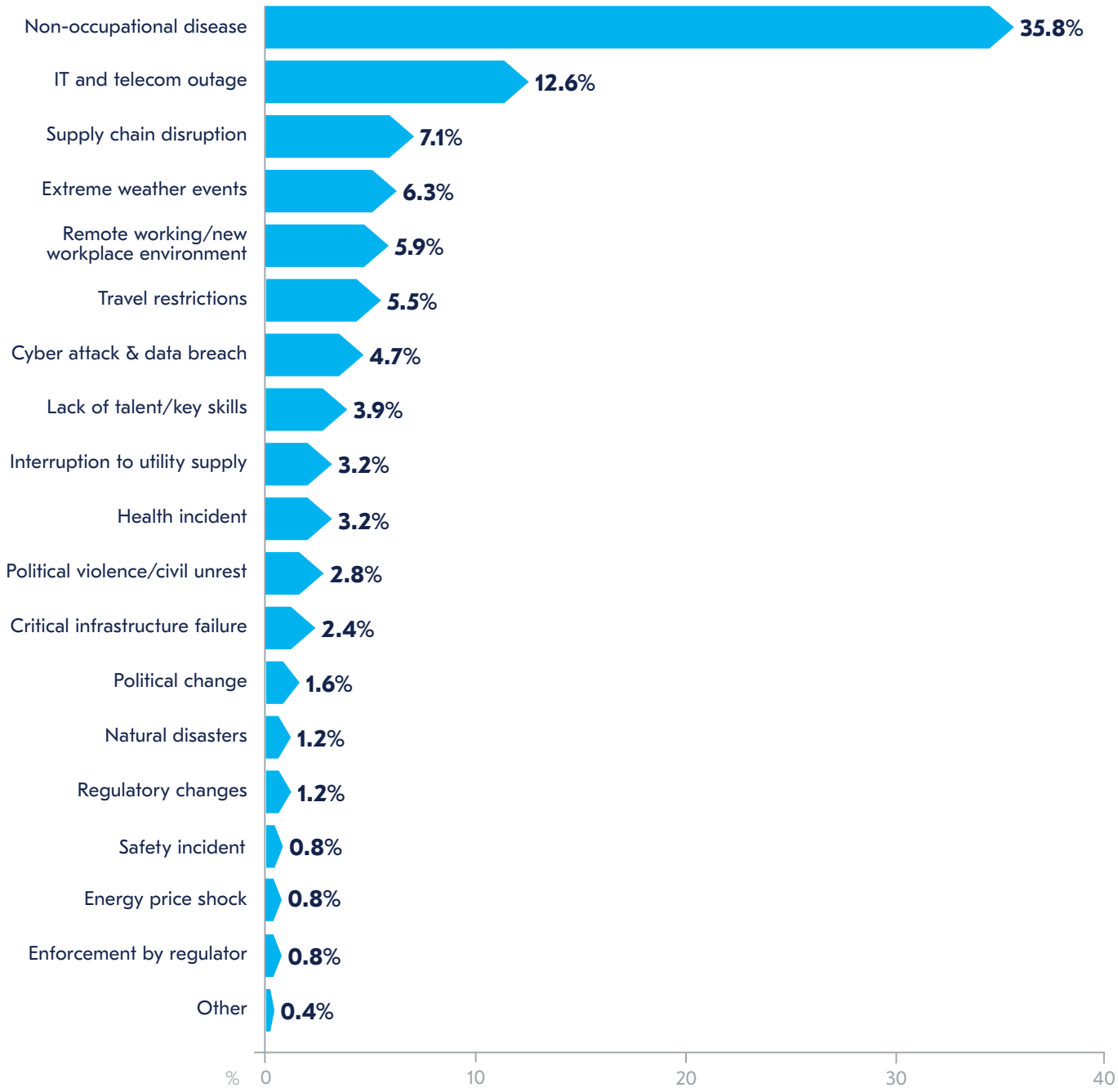


Figure 2. Please indicate below which of the above event was your most major disruption in the past year:

Risk and threat assessment: next twelve months

Risk and threat assessment: next twelve months

- **The pandemic remains top of organizations' concerns for 2022 – but is this still now the case with increasing global tensions?**
- **Cyber security strategies will be tested in 2022, with attacks now targeted towards global supply chains.**
- **IT and telecoms outages remain at the top of the list and, with organizations becoming increasingly dependent on a single platform for all communications, there is concern that many do not have sufficient back-up processes in place.**
- **Severe weather continues to be a concern, although most organizations have yet to consider the chronic threat of climate change in their planning strategies.**

Participants reported non-occupational disease as their biggest concern for the upcoming twelve months, with a risk score of 7.8. This is understandable as the world is still suffering from the impacts of the pandemic, and organizations are still struggling to adjust to a new post-pandemic reality.

However, each year we comment on how the risk landscape is changing, but practitioners' concerns continue to divert to those risks to which they have been most exposed to in the previous year. With COVID being considered less of a threat to life in many countries, it might be considered that other incidents may be considered above non-occupational disease in terms of risk mapping. Indeed, interviewees who had selected the threat of 'non-occupational disease' as minor commented that other issues were now taking precedence in their own organizational risk landscapes. On this note, cyber risk is today one of the largest threats and, according to interviewees, is greater than it ever has been. Indeed, the previous section highlighted that cyber-attacks increased by around 50% in 2021 and concerns around state-sponsored cyber-crime and ransomware attacks are high. Starting in the weeks prior to the beginning of the conflict, the Ukrainian government and other public services were hit by distributed denial of service (DDoS) attacks, which caused significant outages within the region.

This resulted in retaliation towards Russia which experienced similar attacks in the days following[12]. As such, cyber-attack and data breach is the second highest concern for the next twelve months, with an overall score of 6.9 (2021: 6.6) and an estimated impact score of 2.2, the highest of the table. The concerns about cyber security are not just held by resilience professionals within organizations, but also by senior management: an interviewee highlighted how their management team was now requesting monthly meetings to receive updates about cyber security issues.

While these risks should not be overlooked, the 2021 *BCI Cyber Resilience Report*[13] has shown that, in the event of a cyber-attack, ensuring that different management disciplines work together is key to a successful response. Benefits include a shorter time of response, better crisis communications and prevention of cyber incidents. Unfortunately, many organizations still experience internal reluctance to true cooperation, as organizational silos are a real hindrance to building true resilience. A truly resilient mindset should consider external threats, but ultimately focus on its internal resources to orchestrate them in the best possible way to protect its critical assets. This is often not the case, and therefore organizations are not well placed to counter modern threats, which leaves ample room for attackers to exploit internal weaknesses.

An interviewee highlighted how the risks associated with cyber security were a critical concern for their organization. They explained that if their systems went down, it had the potential to not only hit consumers, but the wider Australian economy in general.

> **"The attention on cyber security is significant in terms of exercises, board engagement, expenditure and regulatory engagement. That investment is indicative of our position in the market - because if we have a two hour IT outage, we end up being front page news on the mainstream media because of the span of our digital market and penetration across Australia. We are increasingly realizing that if there is an issue with any of the major banks within Australia it has a large impact, not just on our retail customers, but on other institutions and even the Australian economy. The Australian government is also starting to become very aware of this too. We are, however, very fortunate that our board members have extremely good awareness of cyber issues."**
>
> Group Business Resilience Manager, Financial Services, Australia

Removing the risks associated with COVID-19 such as new workplace environments and travel restrictions, IT and telecom outage again appears towards the top of the risk index in fifth place with an overall score of 4.9. Although this is lower than last year's score of 5.2, interviewees unearthed significant concern for IT and telecom related issues in the year ahead. The *BCI's 2022 Emergency Communications Report* demonstrated how most organizations were now using voice-over-IP (VoIP) solutions for their telecommunications systems. Some were even routing all voice calls through Microsoft Teams. Whilst this is might be advantageous from both a cost and systems management perspective, it does open organizations to a two-fold threat: 1) in the event of an internet outage, no voice calls could be made over company phone systems; 2) an overreliance on a service from a single organization (such as Microsoft) could mean all systems fail in the event of a platform outage. This exemplifies the importance of a reliable back-up solution being put in place, although even this has to be researched carefully. Interviewees explained how they were seeking to reinstall copper line into their organizations to have a PSTN backup, but many countries are now looking to remove this traditional method of communication entirely. For example, in the UK, the PSTN and ISDN networks will be switched off in 2025 . Germany, Japan, Sweden, Estonia and the Netherlands have already made the switch — or are imminently about to do so. The target switch-off globally is 2030.

12. Barrett, B. (2022). Security News This Week: DDoS Attempts Hit Russia as Ukraine Conflict Intensifies. Wired.com [online]. 26 February 2022. Available at: https://www.wired.com/story/russia-ukraine-ddos-nft-nsa-security-news/ (accessed 15 March 2022).
13. Elliott, R. & Lea, D (2021). BCI Cyber Resilience Report 2021. The BCI. Available at: https://www.thebci.org/resource/bci-cyber-resilience-report-2021.html (accessed 15 March 2022)

Ranking respectively third and fourth, travel restrictions and remote working, are two additional consequences of the shift in workplace mode caused by the virus. As discussed in the previous section, they have been a challenge in the past twelve months, and they will continue to be in the upcoming year. This shows that professionals are still battling with problems associated with change management, an overlooked topic when it comes to business continuity and resilience. However, in the past two years, the boundaries between change management and the protective disciplines have become increasingly blurred.

Most changes in the workplace now carry some issues in terms of business continuity, whether it is about being able to fly staff to a different country, choosing a new supplier, or allowing a large part of the workforce to operate remotely. Furthermore, now that many organizations are looking to organise themselves in an entirely remote environment or hybrid environment permanently, 2022 will be the year that the foundations will be made for these new working practices going forward. New business continuity plans will have to be built to cater for the new working environment and the organization is likely to face new risks. Embedding these new practices into organizations will take time and there will be some organizations which will face disruption as a result.

Despite not being among the greatest causes of disruption in the past year, extreme weather events, critical infrastructure failure, and regulatory changes all rank as joint sixth with a score of 4.8, making it to the top ten concerns for 2022. Issues concerning weather events and critical infrastructure are of the utmost importance as they also figure specifically among the seventeen UN Sustainable Development Goals, under Climate Action and Industry, Innovation and Infrastructure. Efforts regarding climate change have intensified noticeably in recent years, increasing pressure on both governments and the private sector to prove they are implementing sustainable policies.

Future requirements in the form of regulations and legislations might turn this into an even more significant challenge for professionals. Thus, if organizations want to stay relevant, they need to show that they are acting ethically and that means respecting global efforts towards a more sustainable, fair and equal society. Going forward, whether or not an organization believes that the increase in severe weather incidents is down to climate change or not, organizations will have to be more prepared and consider reviewing severe weather incidents as chronic, rather than acute risks.

An interviewee in the UK explained how Government legislation on sustainability and carbon reporting was going to be a major challenge for them in the short- to medium-term. Furthermore, if legislation was not adhered to, there was the additional risk of losing a director which could invoke significant financial loss to the business.

Another interesting discrepancy between the risk assessment of the last twelve months and that of the year ahead concerns human resources. Lack of talent and key skills ranked ninth, despite being the fifth cause of disruption, meaning that respondents appear slightly more confident in finding the right candidate for internal vacancies in the next twelve months. Similarly, in 2021, health incidents came fourth in the risk index and slide down to tenth place when it comes to future concerns. This is an interesting trend, as the job market is undergoing important changes, with employees reclaiming a significant part of their negotiating power when it comes to their relationship with current or prospective employers. Equally, mental health formed a large component of those who viewed 'health incidents' as a major disruption in 2021. As organizations return to office environments, the assumption might be that mental health episodes reduce. However, in reality there are other risks that can have an impact on mental health — including global geo-political instability. It is important that organizations retain the focus on mental health and wellbeing that was borne out of the pandemic.

We are at a point in time where physical and mental health are becoming a central part of conversations around hiring and retaining skilled staff. In addition, safety incidents only rank as fourteenth for future concerns, despite ranking as sixth in the 2021 risk index. There is a possibility that as organizations return to office environments, safety incidents may reduce as onsite training can return. With new working practices now endemic, new safety guidelines will have to be drawn up, new equipment may be bought which will require additional training and the risks associated with working in a physical environment will return. Therefore, it might be expected that safety incidents would be higher up the risk agenda for 2022.

Historically, staff safety and wellbeing have been less of a priority than they should be as they do not carry a feeling of imminent threat such as cyber-attacks or natural disasters. However, the way management treat their staff will be a success factor going forward. Those organizations who fail to update health and safety policies and procedures face losing staff in favour of those organizations who acknowledge the importance of the health, safety, and dignity of their workforce.

Supply chain disruptions should not be overlooked too as the global supply chain crisis continues and the importance and complexity of this issue fails to attract the right attention. At the start of the pandemic, several organizations fell short of satisfactory supply chain resilience levels. As such, this needs to be a prime focus going forward. Supply chains are the very fabric of the global economy. The ability to ship goods efficiently across countries is the foundation of sustainable international trade deals, which support healthy national economies and provide access to goods — including primary ones — across the globe.

Unfortunately, because they are so embedded in the fabric of organizations, supply chains are also affected by most types of business challenges that are out there. Transportation and shipping can be affected by new regulations, extreme weather events, political violence and, in recent years, by cyber-attacks.

In the last year only, several energy suppliers (such as the US Colonial Pipeline) experienced cyber-attacks, shedding light on the vulnerability of critical infrastructure towards online threats. Organizations should always understand who their critical suppliers are and engage in conversations to increase resilience levels. It is understandably tough to do so through the entire network.

A good first step is starting with Tier 1 suppliers to establish a first line of defence and then cascade through tier 2, tier 3 and beyond. Equally, ensuring that due diligence of suppliers is done at the procurement stage of the process is encouraged. This enables any potential issues to be raised before entering into a contract which can be too late.

An interviewee highlighted that supply chains are a key vulnerability in terms of resilience. For example, if one of an organization's critical suppliers is hit by a cyber-attack, it can have an immediate effect on supplies, which can lead to stalling of production. Such incidents are already happening globally: Toyota announced at the beginning of March that a cyber-attack had affected one of its critical suppliers and 28 lines of production were halted. As a result, the company lost production of 13,000 vehicles[15].

"One are that we are focussing on is supply chain disruption. Recent incidents have shown to everyone how fragile supply chains are. And even with our key suppliers that we work very closely with, there's a degree of uncertainty and lack of control over all aspects. So for instance, if one of our major technology partners who provide critical services to us was to have a major ransomware attack that would potentially have quite a large impact upon us."

Group Business Resilience Manager,
Financial Services, Australia

15. Green, W. (2022). Cyber-attack on supplier halts Toyota production. CIPS [online]. 1 March 2022. Available at: https://www.cips.org/supply-management/news/2022/march/cyber-attack-on-supplier-halts-toyota-production/ (accessed 15 March 2022)

It is important that organizations rely on processes to establish resilience and not only on technological solutions. The introduction of new technology (which ranks twelfth) is an opportunity as well as a challenge. For example, when considering more automated processes, relying on algorithms only can be a double-axed sword as the machine can still be imperfect due to mistakes and biases in the programming phase. For instance, aggregators of large data are great for understanding the big picture of a certain phenomenon, but there may be inaccuracies when it comes to understanding more nuanced events. In this sense, over confidence in large aggregators of business data can be a risk in itself[16]. In addition to this, many organizations found themselves adopting new systems and technologies during the pandemic and are now looking to fully embed them within their organizations. The 2022 *BCI Emergency Communications Report*[17] showed that, during the pandemic, several organizations had bought in new solutions to aid with emergency communication in new work environments, but for 2022, they were concerned that embedding this new technology may lead to unwanted disruption of operations. One interviewee described how their organization had moved over to Google Suite which has helped to make their whole IT infrastructure both secure and adaptive to working in remote environments. Another highlighted how planned software upgrades had the potential to add a risk with severe impact to their organization. In this case, the resilience manager was working with the IT department to ensure several types of hosting environments were present to mitigate that risk.

"The more interconnected you make the networks and the way that we do business, the greater influence any breach can have within the day to day running of a business. Traditionally, it would have been in much more segregated from the outside world than it is today."

Resilience Professional, Utilities, United Kingdom

"One of our major concerns is IT, especially with the possibility of an outage. We've got a lot of proprietary software which we are upgrading at the moment. Because you're messing with the system, there's the possibility that it can go down. We have found that this has happened a lot – with a significant impact – but enough to stop our staff working for a number of hours. We can't afford to lose that much time and the impact to us is moderate to, at times, severe. We've always kept IT alert to this fact, and we now have other data centres, as well as extra servers on site. We're also building different types of environments."

Senior Business Resiliency Manager, Healthcare, United States

16. Laney, D.B. (2022). A Lesson In Flawed Metrics Design: The New Global Supply Chain Pressure Index. Forbes [online]. 6 January 2022. Available at: https://www.forbes.com/sites/douglaslaney/2022/01/06/a-lesson-in-flawed-metrics-design-the-new-global-supply-chain-pressure-index/?sh=5b61b89a2431 (accessed 15 March 2022)
17. Elliott, R. & Lea, D. (2022). BCI Emergency Communications Report 2022. The BCI. Available at: https://www.thebci.org/resource/bci-emergency-and-crisis-communications-report-2022.html (accessed 15 March 2022)

Legacy software still remains an issue within some organizations, particularly where systems had had updates delayed in recent years. One interviewee highlighted this was now an issue for them, particularly when coupled with the global shortage of silicon chips as they were now having difficulties acquiring new hardware.

> **"One of our issues is the global shortage of chips as it means that we might have to continue dealing with legacy equipment for the time being. Legacy equipment tends to cause a lot of disruption in the IT environment because technology capacity, demand from customers and demand for data storage, tends to increase. So the shortage of chips is something that will start impacting us as businesses."**
>
> Head of Continuity Management, Financial Services, Zambia

Rank	Event	Likelihood	Impact	Risk score
1	Non-occupational disease	3.9	2	7.8
2	Cyber attack & data breach	3.1	2.2	6.9
3	Travel restrictions	3.5	1.6	5.6
4	(Issues arising from) remote working/new workplace environment	3.6	1.4	5.0
5	IT and telecom outage	2.9	1.7	4.9
6	Extreme weather events (e.g. floods, storms, freeze, etc.)	3	1.6	4.8
7	Critical infrastructure failure	2.4	2	4.8
8	Regulatory changes	2.8	1.7	4.8
9	Lack of talent/key skills	2.6	1.8	4.7
10	Health incident (NOT transmissible disease such as COVID but occupational disease, reportable occupational disease, stress/mental health, increased sickness absence)	2.8	1.6	4.5
11	Supply chain disruption	2.5	1.7	4.3
12	Introduction of new technology (IoT, AI, Big data)	2.7	1.5	4.1
13	Natural disasters (earthquakes, tsunamis, etc.)	2.1	1.9	4.0
14	Safety incident (personal injury, fatality, asset damage, dangerous occurrence, reportable incident)	2.4	1.6	3.8
15	Lone attacker/active shooter incident	1.8	2.1	3.8
16	Interruption to utility supply	2.5	1.5	3.8
17	Enforcement by regulator	2.3	1.6	3.7
18	Exchange rate volatility	2.4	1.5	3.6
19	Political change	2.5	1.4	3.5
20	Political violence/civil unrest	2.2	1.4	3.1
21	Energy price shock	2	1.5	3.0
22	Higher cost of borrowing	2.1	1.4	2.9
23	Natural resources shortage	1.8	1.4	2.5
24	Product safety recall	1.5	1.4	2.1

Table 2. Please insert the likelihood and impact levels for each event in the following list that might occur in the next twelve months:

Risk and threat assessment: next twelve months

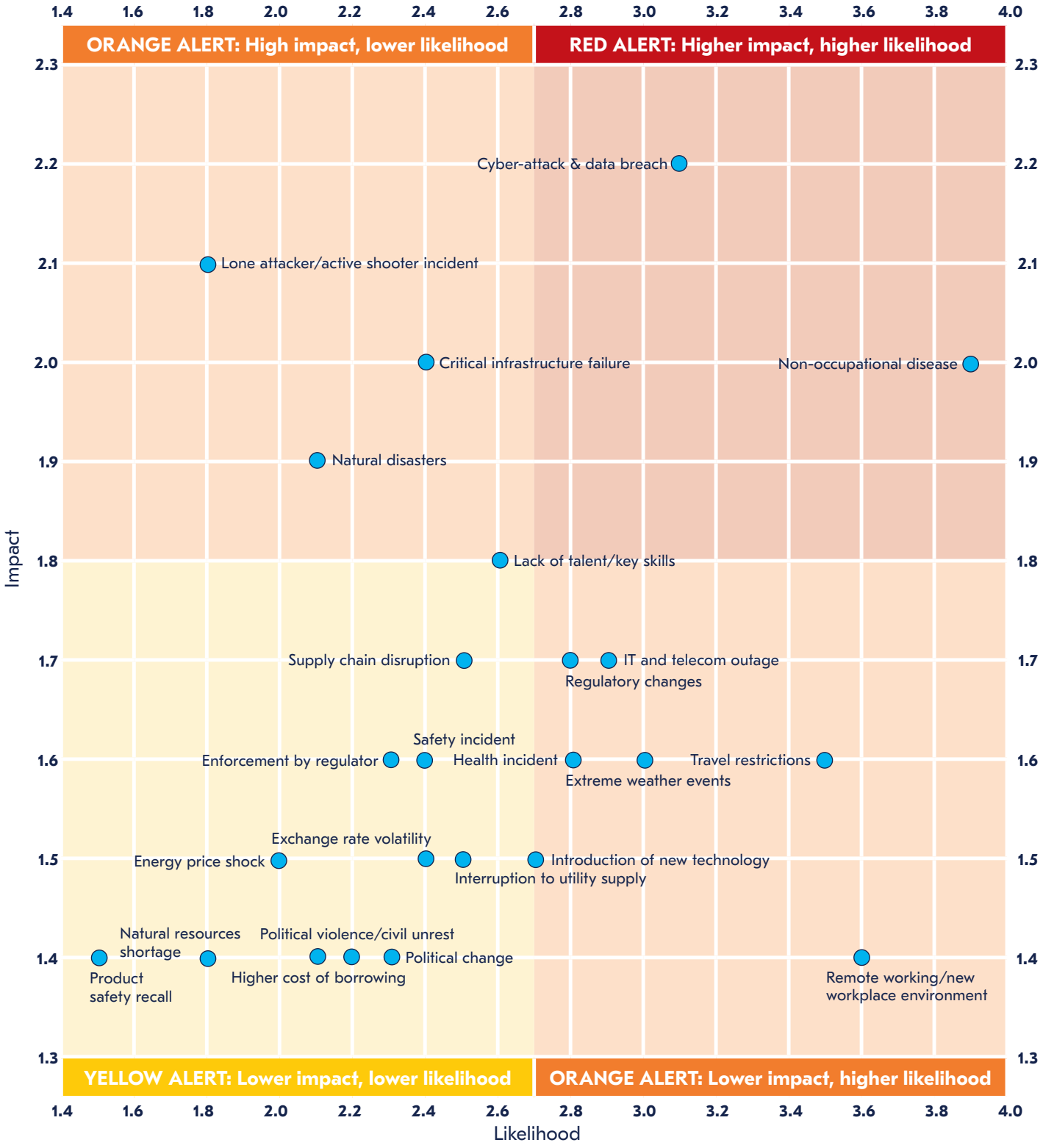


Figure 3. Risk and threat assessment: next twelve months

Consequences of disruption

Consequences of disruption

- **Staff morale, wellbeing and mental health is now the greatest consequence of disruption for organizations demonstrating the increased focus on staff wellbeing programmes exhibited in the early stages of the pandemic needs to continue.**
- **Staff loss or displacement was reported as a major concern by nearly half of respondents showing that the 'great resignation' is a reality for many organizations.**
- **The excuse of COVID-19 as a cause for poor customer service or product/service delays is now wearing thin. Respondents reported rises in customer complaints and reputational damage over the past year demonstrating customers are becoming less forgiving of bad service.**

The two main consequences of disruption for participants are negative impact on staff morale, wellbeing and mental health (68.1%), and loss of productivity (62.1%). The former has risen from second place in the 2021 report to first position in 2022, with an increase of seven percentage points.

The World Health Organization[18] reports that the global economy loses $1 trillion every year in decreased productivity due to mental health issues, which find an unfortunate fertile ground where there is widespread harassment, bullying, and other similar toxic behaviours. In many quarters, the mental health issues that arose from the pandemic - including issues such as feelings of isolation, financial apprehension, job concerns, home-schooling and medical worries - led to the mental health crisis being referred to as the second pandemic[19].

18. World Health Organization [undated]. Mental health in the workplace. WHO [online]. Available at: https://www.who.int/teams/mental-health-and-substance-use/promotion-prevention/mental-health-in-the-workplace (accessed 15 March 2022)

19. Mind (2021). Mind warns of 'second pandemic' as it reveals more people in mental health crisis than ever recorded and helpline calls soar. Mind [online]. 13 November 2021. Available at: https://www.mind.org.uk/news-campaigns/news/mind-warns-of-second-pandemic-as-it-reveals-more-people-in-mental-health-crisis-than-ever-recorded-and-helpline-calls-soar/ (accessed 15 March 2022)

On the brighter side, for every dollar invested in mental health, there is a return of $5 in terms of productivity and better health[20]. However, financial benefits should not be the primary driver in ensuring good mental health policies for staff. It is about making sure that organizations play their part in promoting a fairer and more sustainable way of doing business. Healthier employees make healthier citizens and ultimately more constructive and innovative societies; the ideal scenario for individuals, businesses, and government.

Factors that can affect mental health in the workplace range from a lack of flexible arrangements and unclear health and safety policies, to feelings of exclusion from important business activities. These unsustainable practices can lead to segregation from the rest of the team, creating a negative loop for the person affected. Zooming in on the practitioners taking part in this research, it is worth remarking that those working in high-pressure positions, such as crisis managers or first respondents are particularly vulnerable to mental health deterioration.

Employers can take action to support staff suffering from mental health issues through a series of initiatives dedicated to creating a supportive and non-judgemental workplace. Raising awareness on the topic is a good way to start. This does not have to be done as a classic seminar with a frontal lecture which is likely to lead to workers not feeling comfortable in sharing information, but by building access to confidential channels where they do feel safe. Organizations can also look at success stories and try to replicate those models that worked elsewhere. Innovative ideas to support mental health can also come from feedback from the employees themselves. Furthermore, employers should appoint skilled professionals or give employees access to initiatives such as Employee Assistance Programmes (EAPs) that can maximise the organization's efforts in supporting mental health[21]. Many organizations did start this during the pandemic but should ensure they continue to offer and promote assistance schemes, particularly as the current global instability is likely to add to mental health pressures.

On a similar note, participants reported staff loss or displacement as one of the main consequences of disruption (44.3%). This report has already touched upon the topic of attracting and retaining top talent, which has become a predominant issue in the past two years. Managing resilience also means checking in with staff and evaluating the impact on highly skilled individuals. While key employees do bring an added value to the organization, they can also represent a single point of failure or an unacceptable concentration of risk. It is good practice for managers to seek to understand what the impact on production would be of losing a specific employee or, in some cases, a whole team.

Business continuity professionals will usually evaluate critical processes and services when performing a business impact analysis (BIA). It is also key that they identify critical members of staff. Any organization should be able to survive the loss of an employee whether that be for health reasons, moving to a different region, being headhunted by a new company or retiring. Effective ways of avoiding a loss of knowledge can be ensuring training takes place to replicate skills or having someone shadow an employee so that knowledge relating to a critical role can be shared. This type of prevention would also work in countering loss of corporate knowledge which was also an issue for almost a third of all respondents to this question (31.1%).

The myriad of incidents which occurred in 2021 caused a loss of revenue for 43.0% of organizations which ranks it fourth in the list of consequences. COVID continued to weigh on many organizations' profitability in 2021 as spending patterns changed and supply chain issues impacted organizations' ability to get products to market.

Supply chain disruption itself rounds up the top five with a 41.3% consensus among participants. Customer complaints in sixth place (39.2%) also prove to be quite a hindrance to business continuity. They rank one place higher with a seven-percentage point increase from the previous year. It seems that the difficulties organizations have been enduring for the last two years do not serve as an excuse in the eyes of the public who still expect products and services to be available. Whilst consumers and businesses were more sympathetic to poor service and a lack of availability of supplies in 2020, the mood turned more to aggravation in 2021 as people believed that organizations should, by now, have addressed any poor service or supply issues which emerged at the beginning of the pandemic.

20. World Health Organization [2020]. World Mental Health Day: an opportunity to kick-start a massive scale-up in investment in mental health. WHO [online]. 27 August 2020. Available at: https://www.who.int/news/item/27-08-2020-world-mental-health-day-an-opportunity-to-kick-start-a-massive-scale-up-in-investment-in-mental-health (accessed 15 March 2022)

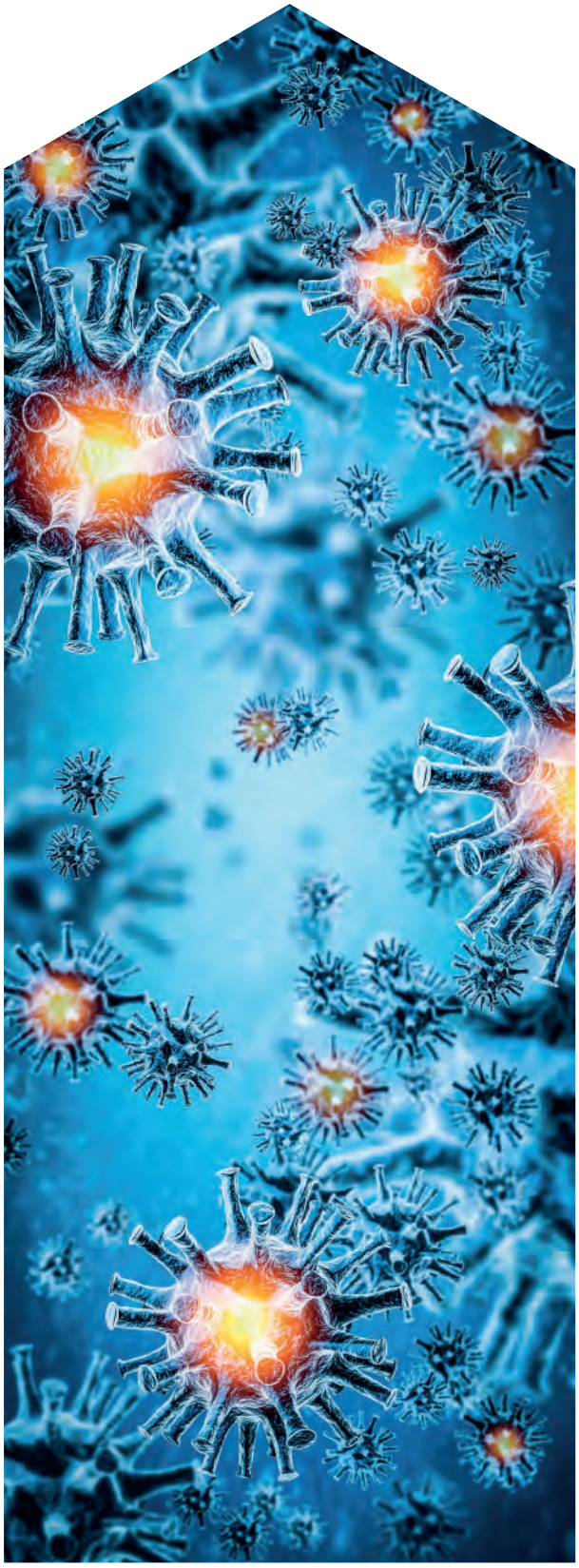
21. World Health Organization [undated]. Mental health in the workplace. WHO [online]. Available at: https://www.who.int/teams/mental-health-and-substance-use/promotion-prevention/mental-health-in-the-workplace (accessed 15 March 2022)

A survey by the Institute of Customer Service[22] found that complaints have reached a record high during the pandemic, with the 'COVID-19 excuse' becoming tiresome amongst the consumer audience[23]. From the customers' perspective, this shows that continuity is not a nice-to-have but a must-have. Perhaps even more importantly, the survey revealed that participants were willing to pay higher prices for a reliable delivery. This sheds light on a very important aspect of resilience and business continuity, that of competitive advantage. Top management often considers such efforts too costly and mainly reactive, whereas the public is explicitly telling the opposite. Those who can deliver — no matter the conditions — will stay in the market, the others will struggle.

This is further confirmed by the fact that one in five respondents (22.1%) experienced reputational damage in the last twelve months. This highlights the usefulness of implementing a business continuity management system, which includes the formation of a crisis management committee or an incident response structure with crisis communications an integral part of the structure. The way management respond and communicate during an incident or a crisis has a significant impact on reputation. Therefore, it is important that executives are ready to speak in a consistent and structured way, avoiding conflicting or false statements.

"During times of disruption, there's normally a time when the customer doesn't receive a service. So during COVID was a period where you find some customers complaining. We had two alternating teams that quickly came in and started sending communications to various levels of customers, so it was individualized communications. As a bank, we've got a certain customer that they're segmented. So you can't just send a one size fits all kind of various customer segmentations so you have to send out different communications depending on the profile of customer. If it is done right, the customers become your ambassadors in championing your response and supporting you during disruption, so that's the one area we have worked on heavily. As a result, we saw a number of customers supporting us, helping us, and lobbying for us on that space."

Head of Continuity Management, Financial Services, Zambia



22. Sky News (2022). Consumer complaints about business reach record high in UK due to COVID shortages. Sky News [online]. 25 January 2022. Available at: https://news.sky.com/story/consumer-complaints-about-business-reach-record-high-in-uk-due-to-covid-shortages-12524477 (accessed 15 March 2022)
23. Peachey, K (2021). Customers fed up with Covid excuse for bad service. BBC News [online]. 7 July 2021. Available at: https://www.bbc.co.uk/news/business-57734808 (accessed 15 March 2022)

In seventh position, increased cost of working ranks lower than last year with a score of 37.9%. Last year, this was in fourth position, and was seven percentage points higher. This is likely to have been down to the higher adoption of remote work, the initial outlay associated with new hardware and software, as well as investment in staff health and wellbeing. The rest of the top ten is completed by two impacts, namely impaired service outcome (30.6%) and increased regulatory scrutiny (22.6%) that both affected a larger number of organizations in 2021, albeit by small margins. Indeed, the interviews carried out for this year's report also show that regulatory concerns were elevated this year, particularly within financial services organizations worldwide.

Which of the following impacts or consequences arose from the disruptions experienced in the last 12 months?

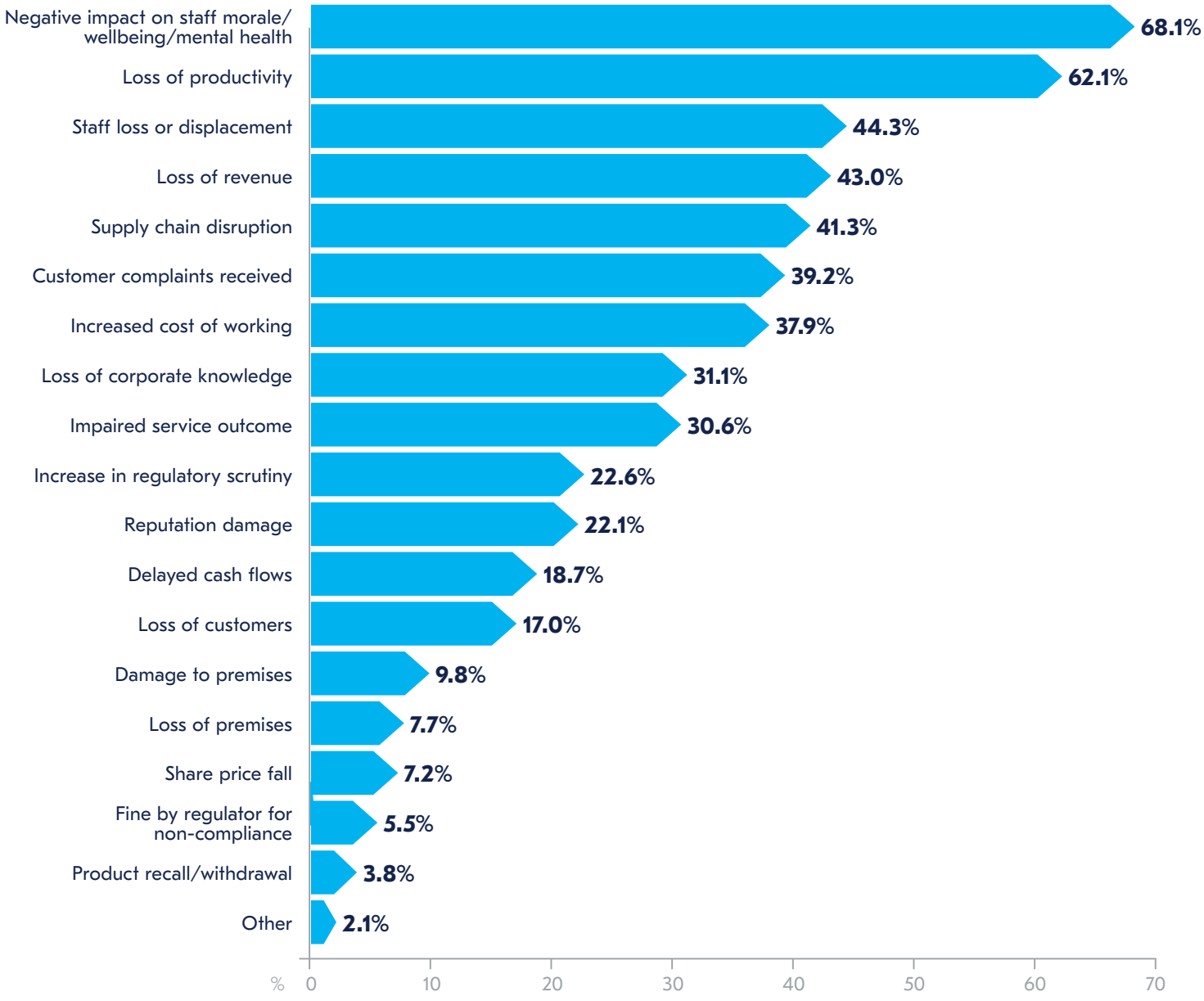


Figure 4. Which of the following impacts or consequences arose from the disruptions experienced in the last 12 months?

Benchmarking business continuity

Benchmarking business continuity

- **ISO 22301 remains the business continuity benchmark for nine out of ten organizations.**
- **Although certification levels fell slightly during 2021, the number of organizations using ISO 22301 as a framework increased by 11 percentage points over the year.**
- **Although organizations report ISO 22301 helps increase organizational resilience and better manage incidents, many cite that it benefits their organization externally: it allows them to demonstrate the effectiveness of their business continuity programme, aids relationships within supply chains and helps to align with industry peers.**
- **Cost remains a deterrent to certification for many companies, although interviewees reported that with the experiences of the pandemic, management teams were pressing for certification for the first time.**

Despite many organizations looking to move beyond business continuity towards overall organizational resilience, the main standard of reference for business continuity professionals remains ISO 22301. 91.3% of professionals say that over the past two years they have not moved away from the standard in favour of another resilience standard (such as ISO 22316). However, types of alignment tend to vary across organizations. Although some interviewees cited that ISO 22301 was becoming less relevant for their own organization, there is a notable increase in the number of organizations who are using the standard as a framework, even if the number who certify has fallen slightly. 63.6% of respondents are using ISO 22301 as a framework (2021: 52.7%) even though they have no formal certification and, of those, 13.5% are currently in the process of getting certified. Additionally, some 7.6% of organizations who currently do not use the standard as a framework, admitted that they plan to move towards it in 2022. Despite the fall in certification this year, nearly one in six organizations are still certified: 15.1% are either certified or in the process of becoming certified (2021: 18.9%).

Although certifications are down slightly in 2021, the appetite for certification does still very much remain. Interviewees explained how their organizations had aligned to the certification for the first time in 2021 after management realised the importance of having a solid and demonstrable business continuity programme in place. Practitioners themselves could see the value, but explained how there was no budget to certify, particularly when the organization had already certified towards another standard(s).

Interestingly, one in five organizations (21%) have no plans at all to align to ISO 22301, revealing there is a significant minority of organizations that still prefer to run their business continuity management programs independently. Indeed, one interviewee highlighted that whilst they value the framework of ISO 22301, they felt that building their own programme which went above and beyond that stipulated by ISO 22301 worked best for their own organization.

It is worth noting that not adopting ISO 22301 does not necessarily mean not relying on standards at all. Several practitioners revealed they use a wealth of guidelines to improve resilience levels within their organization. ISO 27001 is one of the most popular documents for resilience professionals as it helps them set up information security management arrangements, focusing not only on the technology, but also on those organizational processes that can boost protection of key data and information. On the same note, respondents report using other frameworks on information security such as NIST, from the US National Institute of Standards and Technology, and COBIT, which is issued by ISACA.

Similarly, the main risk management standard ISO 31000 is another major player in the resilience industry. The 2018 update attempts to make risk management more strategic and embedded within internal processes which makes it possible to use for objectives too: another driver for this standard's popularity. Another takeaway from the update is to dedicate enough resources to risk management and establish clear roles and responsibilities. Following this line of thought, these principles are also very much applicable to business continuity management, particularly as many organizations are moving towards overall resilience.

Moving forward, ISO 22316 tries to tie a variety of management disciplines together to establish organizational resilience. The standard does not emphasize any specific unit or division responsible for this, but it stresses the importance of cooperation and the removal of internal silos. The principles to get to true organizational resilience are somewhat similar to those present in ISO 22301 or ISO 31000, especially with regards to investment levels, raising awareness, and top management commitment. The general trend seems to be to align resilience functions with strategic objectives as much as possible, to avoid perceiving it only as a cost. The findings of this report support this notion, as participants revealed that in the last year, being resilient brought a series of advantages including a more prominent position in the market. Despite this concerted move towards resilience, most organizations are not yet ready to retire their use of ISO 22301 in favour of ISO 22316: just 3.5% of organizations are planning to move towards ISO 22316 as their preferential resilience standard.

Despite the ISO 22301 standard still prevailing in popularity amongst resilience professionals, some organizations are going beyond standards within their organizations to demonstrate exemplary organizational resilience. One interviewee spoke about how they had instigated a joint project with peers, other industries and governing bodies to 'future proof' the resilience of the sector.

"I'm doing a collaborative project with the utility companies to ensure continuity of supply. I'm working with Telstra — the telecommunications company, NBN, internet, water, and all the energy providers. This collaborative groups aim is to undertake tactical planning together. I'm finding that during an actual emergency, the different parts of the cog need to collaborate. This is where the incident management part of my role, and business continuity work quite well together because I'm able to instantly see and then plan exactly what is critical. Bringing the whole utility sector together. It's instigated off the back of a power outage incident in November last year where I realised half the people during the incident didn't know each other and it was a perfect opportunity to collaborate and actually share."

Business Resilience Advisor, Utilities, Australia

In the past year, other standards that turned useful for organizations touch upon different topics, mirroring the risks highlighted in this report, such as health and safety (ISO 45001), environmental management (ISO 14001), incident response (ISO22320), and quality management (ISO 9001).

56.0%
We use ISO 22301 as a framework but are not certified to it.

5.3%
We use ISO 22301 as a framework, are not certified to it, but are in the process of getting certified.

9.8%
We use ISO 22301 as a framework and certify to it.

7.6%
We don't currently use ISO 22301 as a framework but we intend to move towards this during 2022.

21.3%
We don't use ISO 22301 as a framework and have no plans to move towards this during 2022.

Figure 5. If you have a formal business continuity management programme in place, how does it relate to ISO 22301?

Top 10 standards used within organizations (aside from ISO 22301)		
1	**ISO 27001**	Information security management
2	**ISO 31000**	Risk Management
3	**ISO 9001**	Quality
4	**ISO 22316**	Organizational Resilience
5	**NIST Framework**	Information Security
6	**COSO Framework**	Internal Control
7	**ISO 45001**	Health and Safety
8	**ISO 14001**	Environmental Management
9	**ISO 22320**	Incident Response
10	**COBIT**	Information Technology

Figure 3. Do you use any other management system standards to manage risk and/or resilience? If yes, please specify which.

Figure 6. Have you moved away from using ISO 22301 in place of another resilience standard (such as ISO 22316) over the past two years?

An increasing focus on organizational resilience (74.0%) remains the main reason to certify towards ISO 22301. However, this year it shares the top of the chart with being able to demonstrate the effectiveness of the business continuity management programme (74.0%). An interesting point about these results is that the main reason to align to the standard appears to be very practical and rooted in the needs of 'the real world'. However, one interviewee raised a concern that they were frequently asked to 'tick a box' to show they certified to ISO 22301 when they were entering into a contract with a new buyer. They felt that more was needed than just a 'tick box' exercise to improve resilience levels and to prove this to their business partners. The same interviewee further affirmed this by claiming it was 'too easy' to not lose a standard, even if errors had been made.

Nevertheless, the importance of demonstrating that the BCM programme is effective is another consequence that has risen out of the pandemic: being able to guarantee continuity of service has earned a more visible role in commercial partnerships.

The third and fourth benefits — which share the same consensus — are also deeply rooted in practical business needs, as 60.0% of participants acknowledge the 'importance of enabling the management of disruptions' and 'consistent BCM measurement and monitoring'. Enabling faster recovery (54.0%) rounds up the top five, with a slightly greater preference than last year (52.1%). However, there is certainly less concern for benefits which relate to organizations outside their own: alignment with industry peers (46.0%) and helping stakeholders manage risk (46.0%) receive less attention from respondents and both lose three positions this year.

Further down the chart, it is worth noting that a significant minority of the respondents report two impacts of ISO 22301 certification: 'improved communications' and employee engagement' (46.0%), and 'better customer satisfaction' (38.0%). Both benefits are pivotal to a successful organization, particularly since the start of the pandemic as they positively affect the people within the organization and the customer base. This report has already demonstrated how some of the main challenges in the past and upcoming year circle around staff morale and reputation; therefore, it is important to understand how BCM supports the organization in this sense.

What benefits does certification provide to you and your organization?

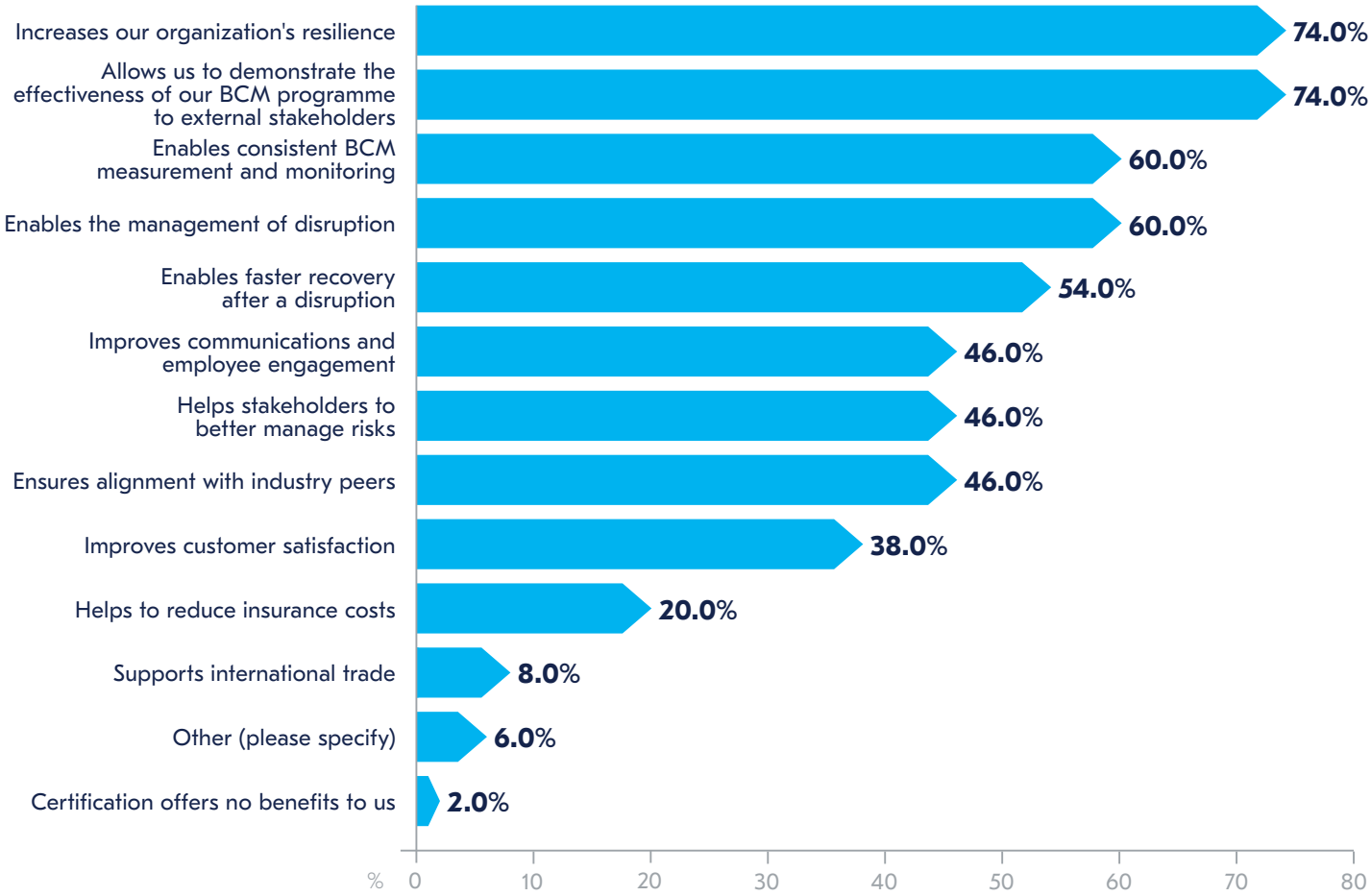


Figure 7. What benefits does certification provide to you and your organization?

Just as last year, 60.2% of respondents did not feel the need to certify due to the lack of business requirements. However, 48.0% state that whilst they are not certified to ISO 22301, they felt very strongly that using it as a framework was important. For some organizations, this is often the first step towards actual certification and, for others, it enables them to build their own resilience models using ISO 22301 as that core part of their skeleton.

On a different note, a significant section of participants admit certification is not relevant to their organization. 29.2% claim there are no external drivers, 26.3% do not see a real value, and a further quarter (24.6%) have no commitment from top management — even though many are working hard to convince management of the importance of certifying.

Nearly a third of organizations (29.3%) also report lack of budget to dedicate to the alignment towards the ISO 22301 standard. This is a similar figure to last year and shows that those professionals who had hope in last year's report of acquiring budget to certify may not have been successful in their approaches to management.

For some countries and/or sectors, ISO 22301 is also less relevant. An interviewee from Ireland explained that ISO 22301 was not widely used in Ireland and, whilst they did use ISO 31000 for some guidance, the business continuity standard was not widely followed at all. They explained how they used the National Framework for Emergency Management instead. Indeed, there are local preferences witnessed globally: in Australasia and the United States, for example, organizations often use locally issued standards in preference to global ones.

"The ISO 22301 standard for Business Continuity does not seem to be in use in Irish higher education. On the emergency management side, we follow the National Framework for Emergency Management, which is similar to the gold-silver-bronze system in the UK. We do not use a standard for business continuity. For Risk Management we follow the ISO 31000 standard for principals and guidelines, I'd like if ISO 31000 was further developed for accreditation and certification."

Business Continuity Professional, Higher Education, Ireland

Another interviewee explained how although the ISO 22301 standard was used as a framework, they did not have time to go through the process of certification due to the good processes they already had in place in the organization around business continuity.

"When we first started our business resiliency plan, it was like most, in Word and Excel, but that was 2015. Trying to be ISO compliant on Word and Excel is nearly impossible. As a result, we've vetted quite a few business continuity software applications and came across a company that had the same ideals that we did. They made sure that their software application was ISO compliant, and it really helped somebody new like me. And so using that application, I believe we are using a great framework. My goal is to get our plans ISO certified one day, but with all the departments that I have – I have to approve 50 different business continuity plans in total – there's just no time to do it at the moment."

Senior Business Resiliency Manager, Healthcare, United States

In fact, all these issues – albeit with some small variation – were also present and relevant last year, showing that there are still many organizations for whom certification is not a viable option now, or in the near future. However, whilst certification is down, we must remember that there is an eleven-percentage point increase in the number who use the standard as a framework, demonstrating that the standard's principles are being adhered to more than ever within organizations.

The conversation around standards and their applicability in the 'real world' is not easy and sometimes quite controversial. The data suggests that there is not a clear division between those who find ISO 22301 and other standards useful, and those who dismiss it completely. Rather, there are different shades of alignment towards international guidelines, that vary due to personal and organizational convictions, budget, awareness, and industry alignment. Alignment and certification should be viewed as a path made of different steps and not with an 'in-or-out' perspective.

At the same time, in the interest of raising awareness, it is important to acknowledge that this report highlights several instances where the practices that are present and recommended by ISO 22301 proved useful during the pandemic. These findings do not rely on speculation or estimates, but they are a direct account of the positive impact of the practices present in documents such as ISO 22301 and the *BCI's Good Practice Guidelines*[24] on the benefits of employing improved resilience tactics.

24. BCI, The. Good Practice Guidelines (2018 edition). The BCI. Available at https://www.thebci.org/resource/good-practice-guidelines--2018-edition-.html. (accessed 15 March 2022)

What are your reasons for not being certified or having no plans to be certified to ISO 22301?

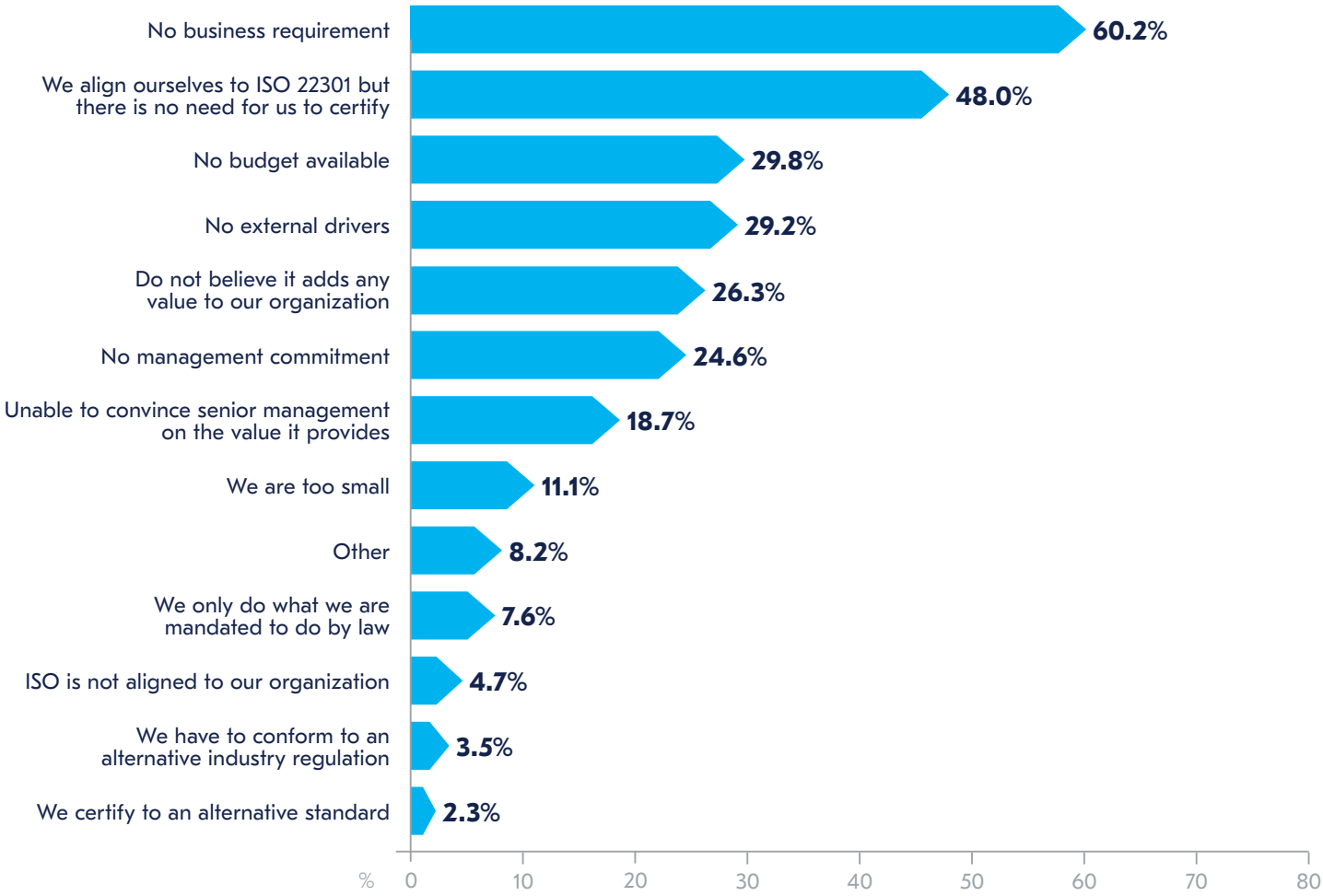


Figure 8. What are your reasons for not being certified or having no plans to be certified to ISO 22301?

Benchmarking longer term trend analysis

Benchmarking longer term trend analysis

- **In the mid- to long-term, cyber-security was cited as a top concern by 85% of practitioners.**
- **Climate risk is an emerging risk, with worsening extreme weather and elevated concerns arising from COP26 encouraging practitioners to consider how climate change will affect their organization in the long term (chronic) rather than short term (acute).**
- **Less than half of organizations have centralized their risk scanning processes, with many labelling it as an 'area cited for improvement' during 2022.**

For the first time in this report, we asked practitioners what their greatest concerns were for the medium- to long-term (the next 5-10 years). Cyber-security was the most prevalent concern, with 85.0% of respondents believing this is the biggest long-term threat to their organization. This concern may have been ranked even higher had the survey period for this report been later: interviewees highlighted how the current situation in eastern Europe had elevated the risk of cybercrime for their organization.

The sheer volume of digitization concerns practitioners, who see the attack surface getting constantly broader as the opportunities for cybercriminals multiply. Current global investment levels in cybersecurity stand at $217 billion, and by 2026 they are projected to experience roughly a 60% growth, reaching over $350 billion[25]. As experts often underline the importance of the human aspect of cybersecurity, the success of a cyber security strategy can be more down to increased training, raising awareness, and promoting best practices in the field than it is to having the most advanced antivirus technologies installed. Indeed, business continuity management is an effective ally in preventing, responding and recovering from cyber-attacks, and it would be wise for organizations to dedicate it part of their budget to training and exercising — as well as technology - if they want to build a truly resilient cyber strategy.

25. Statista (2022). Size of the cybersecurity market worldwide from 2021 to 2026. Statista [online]. 14 February 2022. Available at: https://www.statista.com/statistics/595182/worldwide-security-as-a-service-market-size/ (accessed 15 March 2022)

One interviewee expressed how their primary long-term concern for cyber security was the increasing use of social engineering within cyber-attacks — and how criminals were becoming ever more deceiving with their attacks.

> **"Attackers are now taking more of a spearphishing approach to target individuals. So the old school phish from a foreign Prince is now dying as everyone is more educated with them, we're seeing a lot more social engineering and targeted phishes. They'll look at your LinkedIn account. They'll look at your social media account. They'll make a speculative intervention with you. At no point will malicious links be shared or anything like that. But they'll build up that knowledge base or the individual. They'll build up that trust, and then deliver the payload when consistent communications and trust is achieved."**
>
> Resilience Professional, Utilities, United Kingdom

In joint second place, non-occupational disease and climate risk both received a 50.0% consensus from participants. These are both threats that belong to environmental and biological realm, which is once more a wake-up call to rethink the impact of organizations on the ecosystems where they operate. The Harvard Centre for Climate, Health, and the Global Environment[26] highlights how the same factors that increase climate risk are also likely to be risk factors in the spread of new viruses. Actions such as deforestation can destroy natural habitats and lead animal species to migrate, carrying with them germs and infective agents that can spread to other species including humans. Furthermore, research has shown that living in areas contaminated by extreme pollution increases the chance of respiratory complications from viruses such as COVID-19 and SARS.

The Climate Action Tracker, a research group that keeps tabs on countries' efforts towards climate change, also reports there is still a substantial gap between current achievements and the established targets. Out of the 35 countries that produce 80% of total pollution, there are still 12 — including large ones such as Brazil, Australia, and Russia — that did not show any real change with emissions that are still above target.

Whilst many organizations are adopting changes into their practice as part of their environmental, social and governmental (ESG) or corporate social responsibility (CSR) strategies, many practitioners admit to viewing events caused by incidents such as extreme weather as 'acute' risks. This means that a well-practiced and rehearsed plan is invoked in the case of a building being destroyed by a flood, for example. In the long term, however, organizations should start to consider severe weather events as 'chronic' risks (e.g. moving a factory if it is on a floodplain, moving offices if they are located in an area prone to wildfires). Some practitioners are already considering this in their own organizations, but interviews for this report suggest that the practice is rare. One interviewee discussed how the questions around chronic climate risk were serving as a prompt to take the case to senior management.

> **"We are definitely looking at sustainability, but I think that's just part of being a good company with strong ethical values. Our location strategy to mitigate against longer term climate change is a really interesting point though. It's not something we've discussed, but I think I will now raise this as an issue. When we are looking for long term, you want a company that can continue, and as these environmental impacts start, you need to be prepared and think about things like office locations in advance."**
>
> Senior Business Continuity Manager, Electronics, United Kingdom

26. Harvard TH Chan School of Public Health (2020). Coronavirus, Climate Change, and the Environment. A Conversation on COVID-19 with Dr. Aaron Bernstein, Director of Harvard Chan C-CHANGE.Harvard TH Chan. Available at: https://www.hsph.harvard.edu/c-change/subtopics/coronavirus-and-climate-change/ (accessed 15 March 2022)

Technology and telecoms failure (35.8%) is the fourth main longer-term risk for practitioners, which is in line with the critical role of IT infrastructure in current times, especially as new hybrid work environments become more popular. Furthermore, new technologies are entering onto the scene at pace and, for each introduction of a new technology into an organization, new training programmes will need to be set up and initial teething issues could lead to failure. There is also the issue which was raised at the start of the report: that of an overreliance on the internet for communications. VoIP might be a cost efficient and convenient solution, but what will happen if the internet goes down or an entire platform, such as Microsoft, is hit by a cyber- attack and all applications — including tools such as Teams — go offline? Such scenarios require considerable planning and back-up processes need to be built in, particularly with copper telephone wires due to be grandfathered globally by 2030.

Moving further down the table, talent concerns (31.4%) and supply chain risk (30.1%) jointly occupy the fifth and sixth place in the table respectively. Both have recurred through the findings of this report and they appear to be here to stay, especially if coupled with other challenges such as regulatory changes (28.3%), adapting to new way of working (21.7%), and geopolitical violence (21.7%).

Some organizations were considering the far broader risk landscape when it came to understanding mid- to long-term risks. An interviewee from the education industry told how they were trying to understand how the industry would evolve over the years, and the challenges they would face on that journey rather than tackle the long-term landscape segmented risk approach. Another interviewee discussed how they prefer to look at the impact of incidents, rather than the cause.

"The major threat on the horizon for us is around the broader picture of academia. What is the future of academia? We also make sure that people are actually thinking about that at the right levels as well. This means I am immersing myself in all levels in the organization, right from the board all the way down to lower grade manual staff. When I started this role, it was about me coming in and going, 'Let me look at everything and understand what it looks like, and then target specifically what the risks are."

Risk & Compliance Officer, Education, Australia

"One thing we always look at is the impact rather than the cause. So the biggest impact for us at the moment is trade compliance and being able to trade freely across the globe. I don't think it matters if it's political change, a war or conflict or something else that's causing it. That's what we're seeing at the moment in Russia. At the moment, it's going to stop us being able to trade with other companies in other parts of the world. That, to me, is an impact."

Senior Business Continuity Manager, Electronics, UK

Comparing the list of risks and threats across different time spans, issues concerning the pandemic (e.g., non-occupational disease, travel restrictions) and the management of human resources (e.g., remote work, lack of talent) are consistently present in the charts for the past twelve months, next twelve months, and next five years. Differently, cyber threats, IT failure, and climate risk become more prominent moving forward. Overall, it is fair to argue that the challenges for organizations in the medium to longer term will fall under three main domains, namely human resources, digital assets, and environmental impact.

However, it is worth highlighting the importance of 'preparing for the unexpected'. Both the 2020 and 2021 Horizon Scan Reports demonstrated that practitioners' concerns for future risks divert to those that they are currently experiencing. This year, this was exemplified in interviews where practitioners admitted that if they were to complete the survey now, cyber security would be rated as a greater long-term risk, due to the escalating situation in Ukraine. Practitioners therefore need to continue to keep a broad view of the risk landscape. Those that use all the intelligence they can to help plan their own risk landscapes will ultimately be better prepared for previously unforeseen incidents that can cause challenges to their organizations. One interviewee was keen to point out that they felt their organization was 'prepared for anything'. When considering future risks, the interviewee had ticked every incident type as 'imminent' such was their preparedness for all types of event.

"Realistically, we are always prepared for unknown incidents. We've got that many incidents going on at any one time, or we've experienced something similar in the past. The team are trained for incident management are very good at responding it's fascinating to watch them. We exercise intensely, probably over and above what we've delivered. For some of the incidents, staff made comments about how the scenarios were far-fetched, and I countered them by explaining they weren't. Then we might have an incident that's similar, but not as intense as what we've used in the exercise scenario."

Business Resilience Advisor, Utilities, Australia

One of the problems is that organizations continue to have a 'reactive' strategy to incidents, rather than being 'proactive' with their approach to planning and thinking longer-term. An interviewee highlighted how management within their organization still preferred to take the former approach, and the resilience manager was trying to get them to move their thinking towards the latter.

"There's a culture within the company around what risks really need looking at and whether there needs to be analysis and communication around it. Currently, they are just at the point where they don't want to be proactive. They're very reactive about incidents. This means, right now, it is really hard to properly plan. So, one of the things I'm working on is trying to get management to be more proactive. They need to be ready for a situation rather than reacting when it happens."

Senior Business Resiliency Manager, Healthcare, United States

However, sometimes a reactive strategy does need to be deployed, particularly in the case of an incident for which intricacies could not be seen in advance. COVID-19 was an example of this, and to some extent, the escalating situation in the Ukraine as well. One interviewee explained how they were already dealing with issues relating to the Ukraine crisis within their own organization.

"We did an assessment of our people and we've had a couple of contractors who are from the Ukraine, so we had to ensure that they are okay. We also have people who work with us from different countries and check that they were not in the region. Similar with Russia and people working in surrounding countries. There's also the internal communication piece and managing what our colleagues are saying to one another and making sure that, whilst people can speak freely, the right things are being said. We also did a full assessment on all our critical vendors to make sure that they're able to deliver to us and what are the impacts to them. We also have to consider our political stance."

Senior Business Continuity Manager, Electronics, United Kingdom

Other organizations stressed the importance of regular after-action or post-incident reviews to ensure learnings made from incidents are quickly embodied into operational plans. An interviewee spoke how they were ensuring there were solar-powered remote terminal unit (RTU) batteries installed in an area which was devastated by a recent earthquake thanks to learnings made from the post-incident investigation.

> **"To mitigate these happening further, we have a post-incident investigation for each incident where we go through what went well, what didn't go well and what we can improve. The endless improvements are then itemized either by documentation updates, further training for people or purchasing products and services. As you can imagine, all the planning we've done in the last couple of years, especially around the power outage planning and comms outage planning, assists us in a lot of the response. We can't mitigate incidents completely from occurring we can just plan for the worst and hope for the best."**
>
> Business Resilience Advisor, Utilities, Australia

Thinking about the next 5-10 years, which are your top three concerns for the mid- to long-term risks?

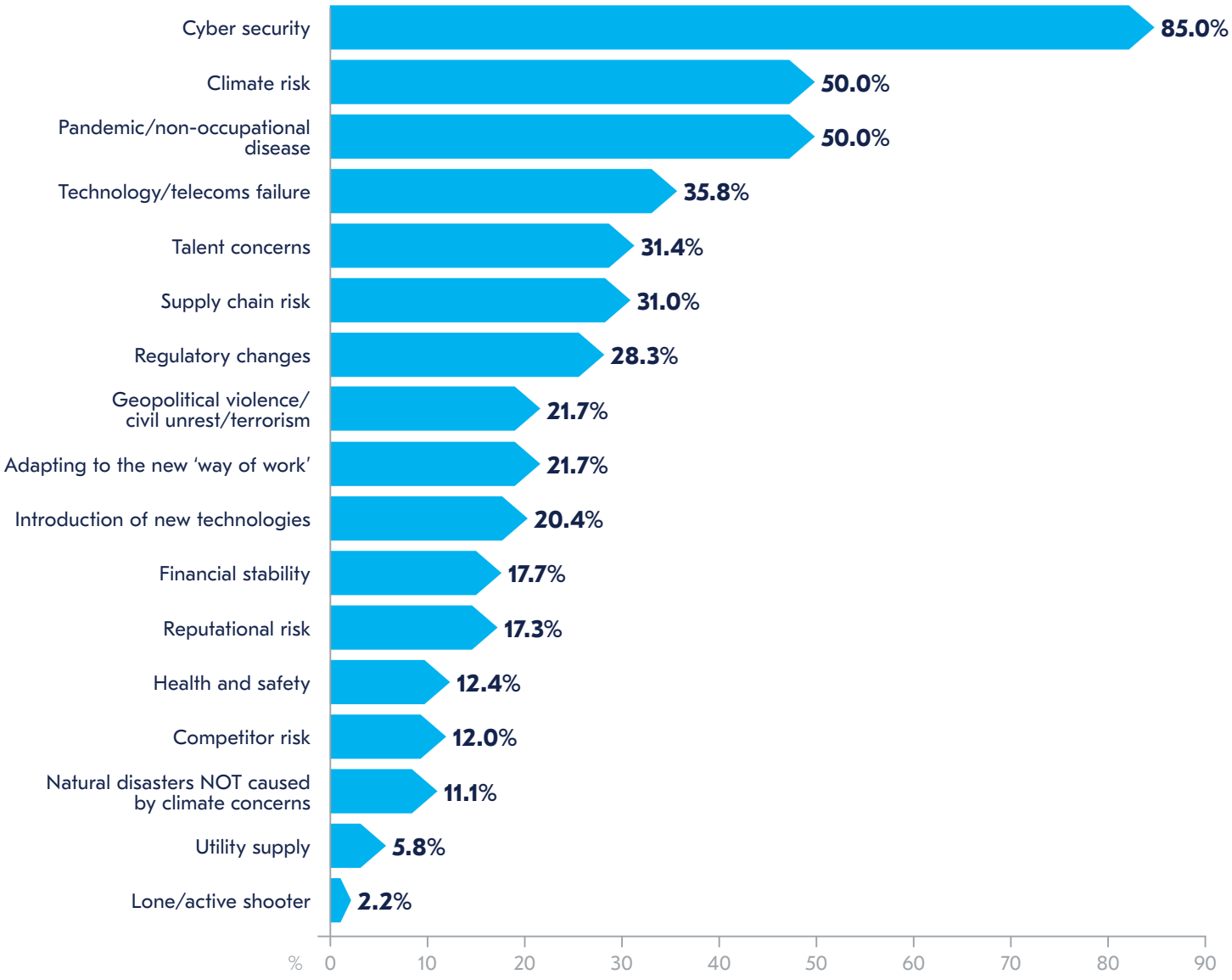


Figure 9. Thinking about the next 5-10 years, which are your top three concerns for the mid- to long-term risks?

Past twelve months	Next twelve months	Next 5 years
Non-occupational disease	Non-occupational disease	Cyber attack & data breach
Remote work	Cyber attack & data breach	Non-occupational disease
Travel restrictions	Travel restrictions	Climate risk
Health incident	Remote work	Technology/ telecoms failure
Lack of talent	IT and telecom outage	Talent concerns

Nearly half of respondents (46.9%) conduct a longer-term trend analysis through a central corporate function or department, while an additional 27.4% do so with the support of many different departments based on specific needs. Disappointingly, both these figures are down compared to the previous year (the 2021 report showed that 52.8% of organizations were now organizing longer-term trend analysis via a centralized function). For many organizations, COVID-19 has been the precipitator for acquiring more data for risk planning processes, centralising these processes and, where possible, investing in data mining processes to help sieve through the information. Although nearly three-quarters of organizations do this, there is still clear room for improvement, particularly given that one in five organizations (20.4%) do not perform this type of analysis at all. Interviews carried out for this report do, however, point to an improving picture. There were several interviewees who commented that they now had a Chief Resilience Officer within their organizations who was looking to drive this kind of process, whilst others had had new senior risk managers employed who had been charged with improving data resources, as well as the mining and management of those resources.

"We are moving forward in terms of resiliency. Resiliency in the organization is very much on trend. We've got a new Chief Resiliency Officer, which we never had before. There's now a more holistic approach to resilience than we've ever had previously. So we're moving in the right direction, but not explicitly aligned to it in any shape yet."

Resilience Professional, Utilities, United Kingdom

"One of the stated aims of our recent departmental organization was to enable a more centralized threat risk and scenario contingency planning. So, for example, when the treasury are looking into liquidity or market funding issues they're working off a consistent view of what the organization sees as the future, as opposed to one department looking at it one way and another department looking at it another way. So, our plans are to centralize that and improve that area within the organization as a whole."

Group Business Resilience Manager, Financial Services, Australia

Whilst organizations may not be as efficient as collecting and analysing data, practitioners are now using the outputs from trend analyses more readily. 52.5% of practitioners state that they draw on the inputs of this trend analysis - an 11-percentage point increase from 2020 — with a further 24.9% who help develop the analysis in the first place. However, there is still a minority (19.1%) of practitioners who do not have access to outputs from trend analyses, albeit down from last year's figure of 24.0%. Not having access does not mean that practitioners are not doing their own analysis. There are a number of free resources available that can help with risk mapping such as the *BCI Horizon Scan*, national risk registers and reports such as the OECD cross-country perspectives on global risk[27].

External forums, conferences and opening up information channels between peers, customers and suppliers can also help to provide useful sources of information.

27. OECD (2022). Risk Governance. OECD [online]. Available at: https://www.oecd.org/gov/risk/ (last accessed 15 March 2022)

46.9%
Yes, this is conducted by a central, corporate function or department (e.g. Business Continuity, Strategy or Risk).

27.4%
Yes, but many different departments do this according to their own needs.

20.4%
No, we don't do this.

5.3%
I don't know.

Figure 10. Does your organization conduct longer term trend analysis to better understand the threat landscape?

52.5%
Yes, I'm aware of the outputs and use them.

24.9%
Yes, I help develop the analysis in the first place.

19.9%
No, I do not have access to this information.

2.7%
No, I don't see the value of this information.

Figure 11. As a business continuity practitioner, do you draw on the outputs of this trend analysis for your programme?

Looking at how organizations perform their longer-term risk analysis, there seems to be a preference to rely on traditional processes more than automated systems. This is not surprising considering that the main tool to gather intelligence remains the internal risk and threat assessment (88.2%) for the second year running. This is the stalwart for risk analysis and it will take years before automated processes replace its effectiveness. The use of external reports and industry insights jumps up in second place - 77.7% of participants include these types of resources in their analysis, compared to 72% last year. This suggests that practitioners are becoming more resourceful in their search for reliable information. Industry research offers remarkable support to professionals in several aspects, such as helping them glimpse the bigger picture while also benchmarking their practices against their industry peers. Being able to access information on what other organizations are doing is a highly effective way to understand the organization's resilience posture and adjust if necessary.

Further down the chart, the duality in the type of information used for the analysis can be noted as risk registers (71.4%) — an internal resource — rank third and the participation to industry conferences and events (62.3%) — which rely on peer-to-peer discussions — are in fourth place. As anticipated, at the bottom of the chart are those solutions that are usually software-based, rely on automation and are more specialist in their application such as social media monitoring (39.6%), automated systems for cyber security (34.6%), and risk assessment software (18.6%).

How do you conduct a trend analysis of the risks and threats to your organization?

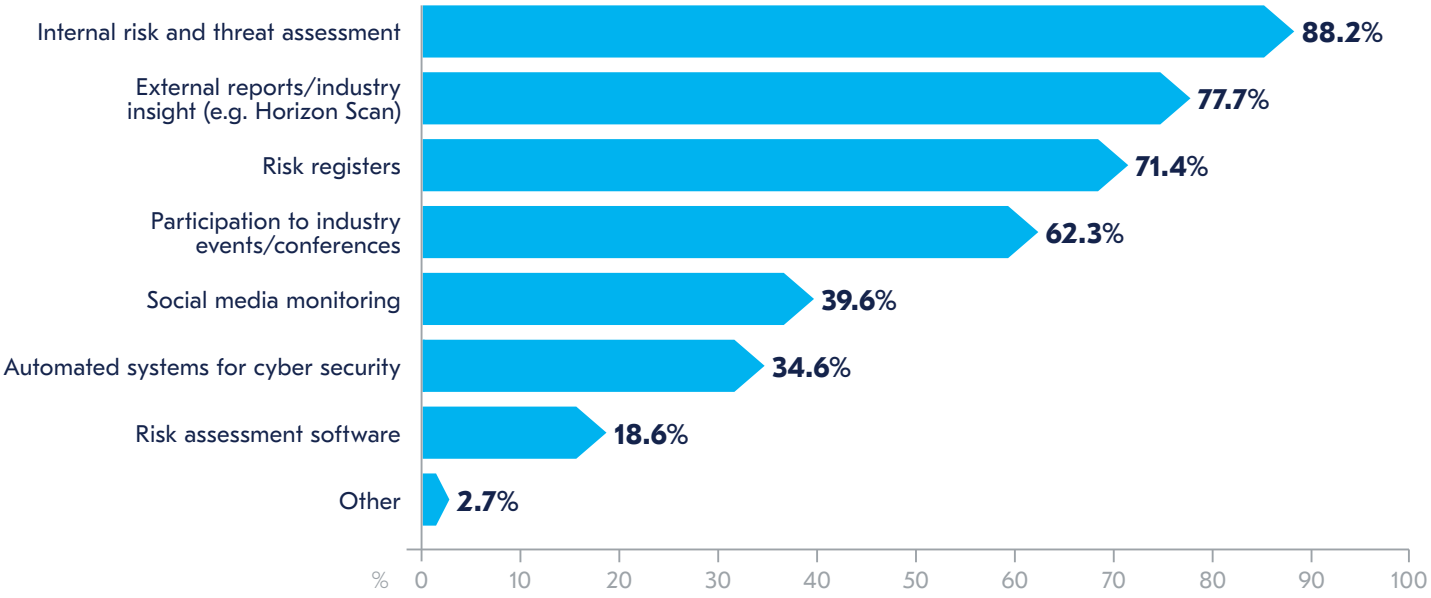


Figure 12. How do you conduct a trend analysis of the risks and threats to your organization?

When it comes to the maturity of respondents' Business Continuity Programmes (BCP), 54.2% report having a mature Business Continuity Management (BCM) programme which has been in place for more than five years, while an additional 39.5% have been engaging in BCM for 2 to 5 years. Only a small minority of them (6.2%) state that this is still new for the business. Compared to last year, fewer participants fall into the 1-year bracket, in favour of more consolidated programmes of 2-3 years. Respondents who report having new programmes is always a positive sign as it demonstrates an increase in the number of organizations who are deciding to employ BCM programmes within their organizations. Furthermore, this group of respondents are not limited to small businesses: some 80% of respondents who report new programmes (<1 year old) are from larger organizations.

A similar trend emerges from levels of investment into BC as more respondents are expecting to have increased budgets this year (33.9% compared to last year's 30.9%). Nearly half of organizations (46.6%) will maintain the same investment levels as last year and only 8.1% say they will cut financial resources for business continuity. While dedicating budget is paramount to a successful programme and a resilience organization, it is also important to remember the other key resource for BCM: people. The *BCI's Business Continuity Resources Benchmarking Report*[28] shows how the most effective BCM functions rely on allies and facilitators throughout the organization, highlighting the importance of embracing a resilience culture and raising awareness.

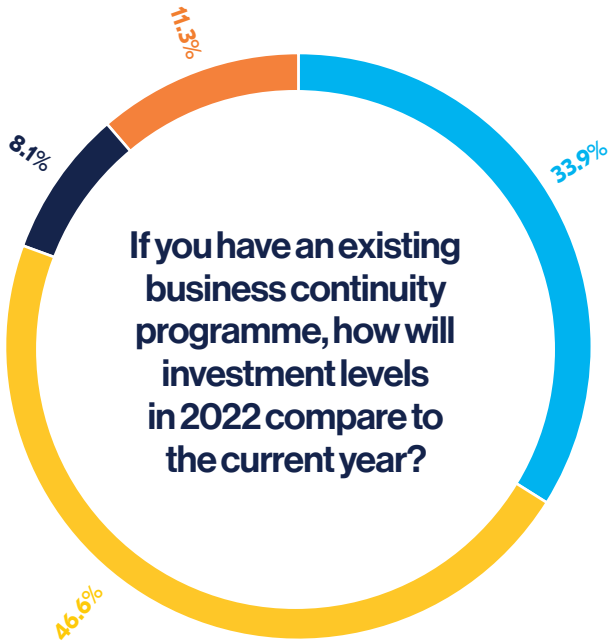
6.2%
1 year — this is still new for the business

21.3%
2-3 years — this has been recently established

18.2%
3-5 years — this is a well-established programme

54.2%
5+ years — this is a mature programme

Figure 13. How long have you been engaging in business continuity management planning for?



33.9%
Investment will be increased to meet the needs of a growing programme or new requirements.

46.6%
Investment will be maintained at appropriate levels for the programme scope and position in the lifecycle.

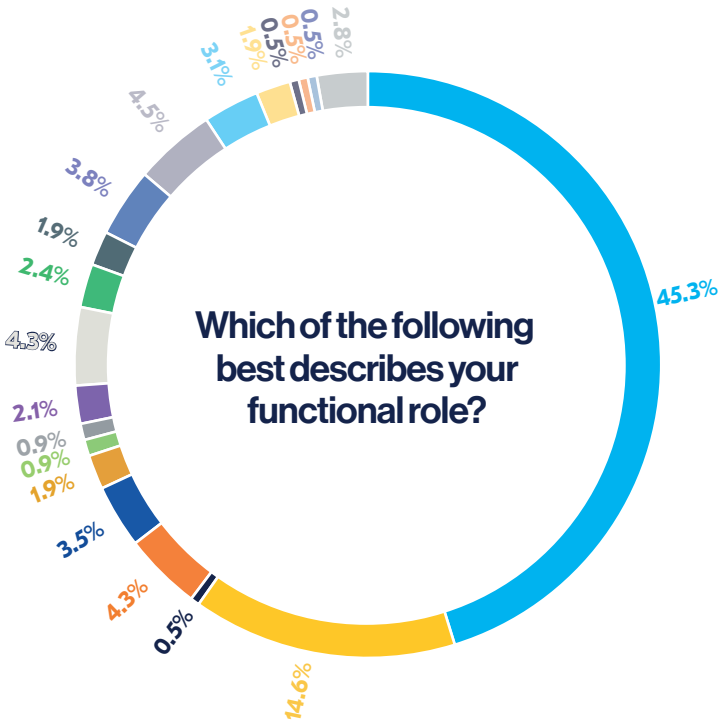
8.1%
Investment will be cut, limiting the scope or effectiveness of the programme.

11.3%
I don't know.

Figure 14. If you have an existing business continuity programme, how will investment levels in 2022 compare to the current year?

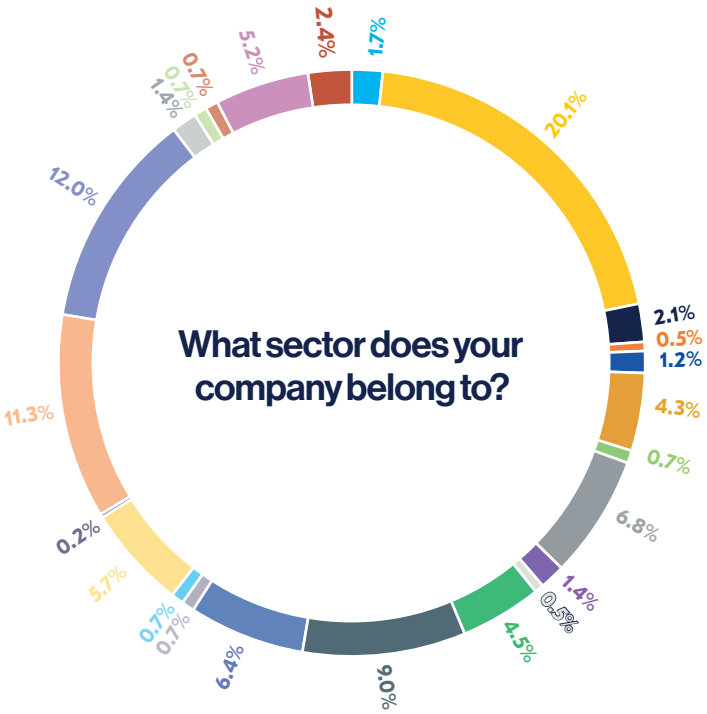
28. BCI, The (2022). BCI Business Continuity Resources Benchmarking Report 2022. The BCI. Available at: https://www.thebci.org/resource/bci-business-continuity-resources-benchmarking-report-2022.html (last accessed 15 March 2022)

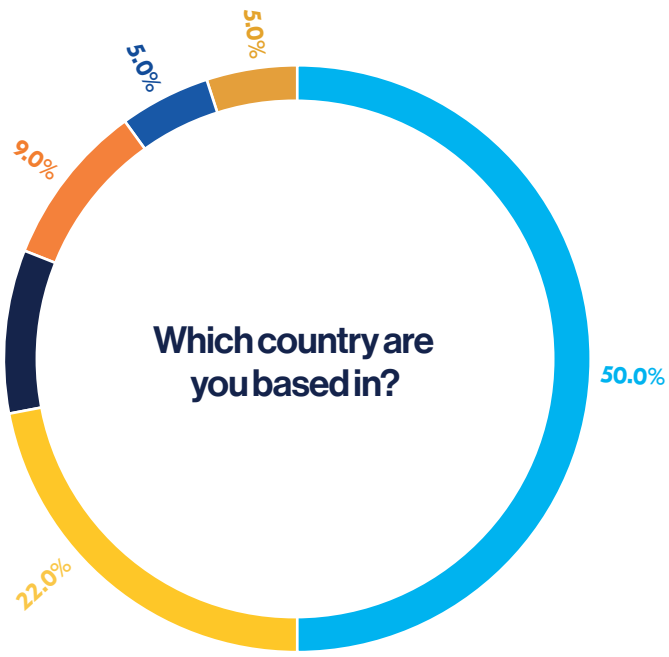
Annex



45.3% Business Continuity	14.6% Risk Management
0.5% Supply chain/logistics/ procurement/purchasing	4.3% Operational Resilience
3.5% Organizational Resilience	1.9% Internal Audit
0.9% Line of Business/ Service Directorate	0.9% Quality/Business Improvement
2.1% Health & Safety management	4.3% Emergency Planning
2.4% Security (physical)	1.9% Cyber/information security
3.8% IT Disaster Recovery/ IT Service Continuity	4.5% Crisis management
3.1% Top management	1.9% Operations
0.5% Human Resources	0.5% Marketing
0.5% Sustainability	2.8% Other

Figure 15. Which of the following best describes your functional role?





1.7% Aviation	20.1% Banking and finance
2.1% Charity/Not for profit	0.5% Consumer goods
1.2% Creative industries	4.3% Education and training
0.7% Emergency services	6.8% Energy and utilities
1.4% Engineering and infrastructure	0.5% Environment and agriculture
4.5% Healthcare	9.0% Information technology
6.4% Insurance	0.7% Law enforcement and security
0.7% Leisure and hospitality	5.7% Manufacturing
0.2% Medical devices	11.3% Professional services (including consuting)
12.0% Public services, government and administration	1.4% Real estate and construction
0.7% Retail and wholesale	0.7% Science and pharmaceuticals
5.2% Telecommunications	2.4% Transport and logistics

Figure 16. What sector does your company belong to?

50.0% Europe
22.0% Americas
9.0% Asia
9.0% Australasia
5.0% Africa
5.0% Middle East

Figure 17. Which country are you based in?

7.1% 1-10

2.6% 11-20

1.9% 21-50

1.7% 51-100

2.8% 101-250

5.2% 251 - 500

8.0% 501 - 1,000

21.9% 1,001 - 5,000

13.7% 5,001 - 10,000

19.8% 10,001 - 50,000

9.4% 50,001 - 100,000

5.9% More than 100,000

Figure 18. Approximately how many employees are there in your organization globally?

7.3% Less than €1 million

7.1% €1-10 million

4.5% €11-25 million

3.5% €26-50 million

5.2% €51-100 million

4.7% €101-250 million

5.7% €251-500 million

5.9% €501 million-€1 billion

13.4% €1-10 billion

8.5% €11-50 billion

5.0% Greater than €50 billion

29.3% I don't know

Figure 19. What is the approximate global annual turnover of your organization?

Asia Pacific: past twelve months

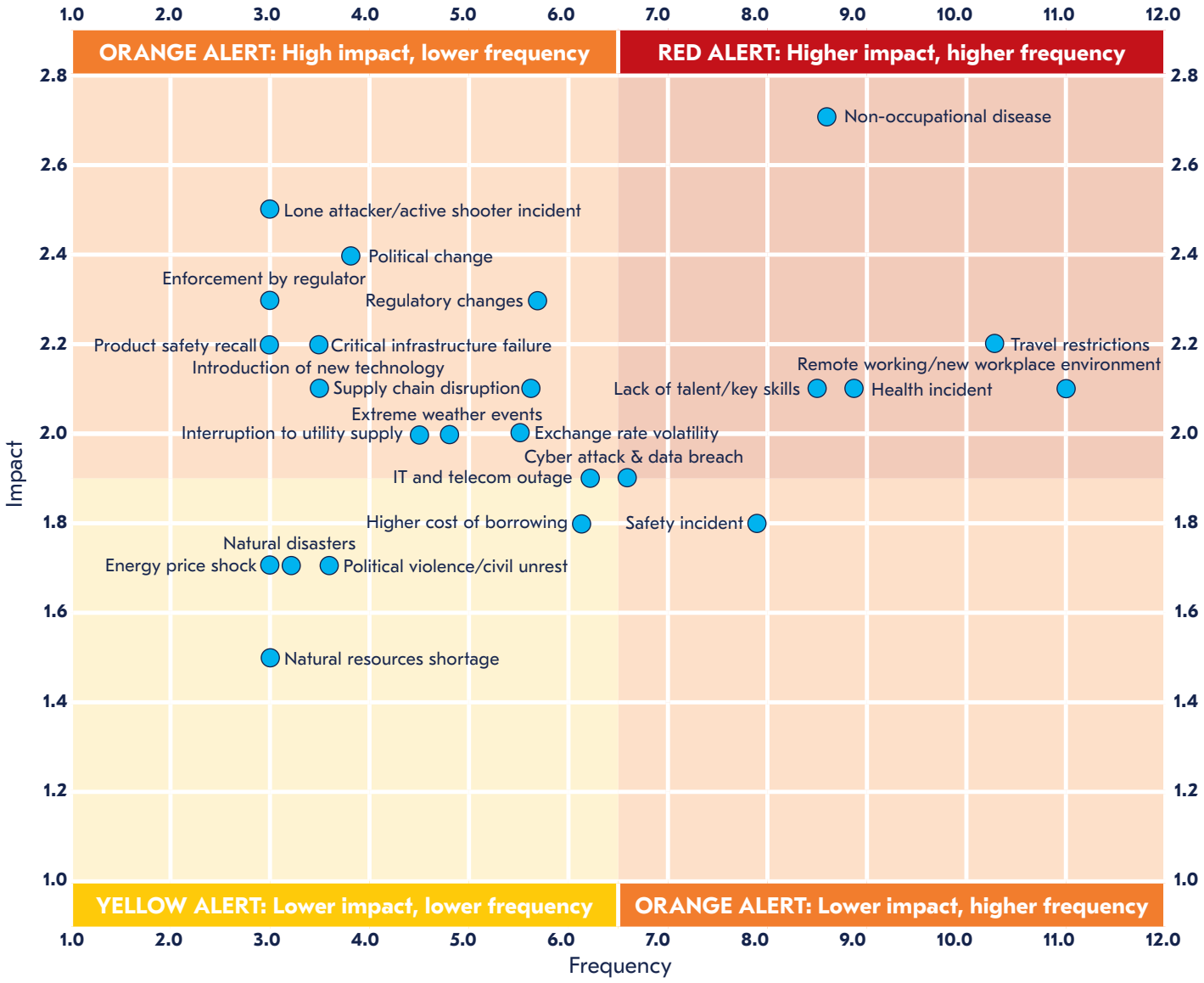


Figure 20. Risk and threat assessment: past twelve months (Asia Pacific)

Europe, Middle East and Africa: past twelve months

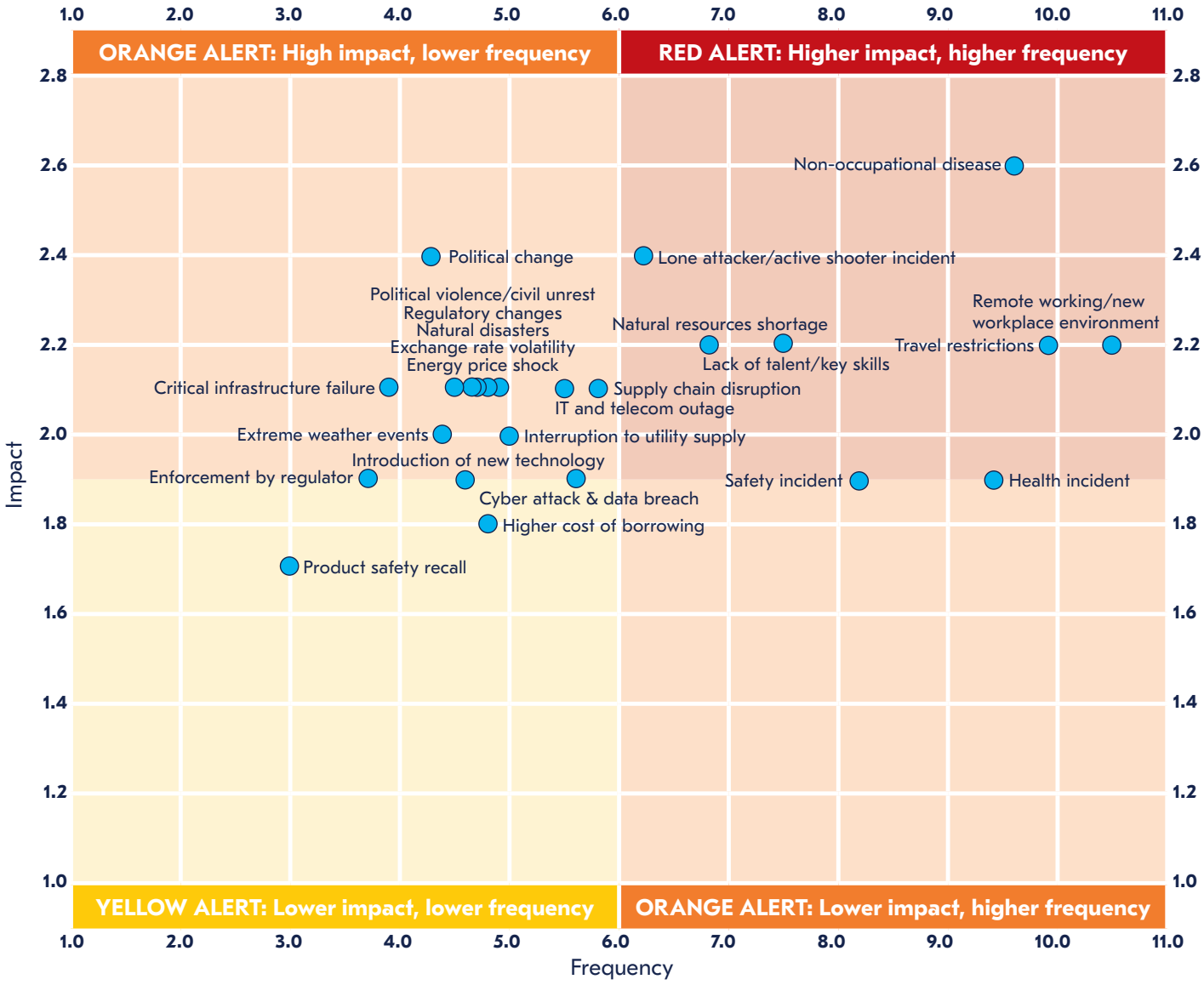


Figure 21. Risk and threat assessment: past twelve months (Europe, Middle East and Africa)

Americas: past twelve months

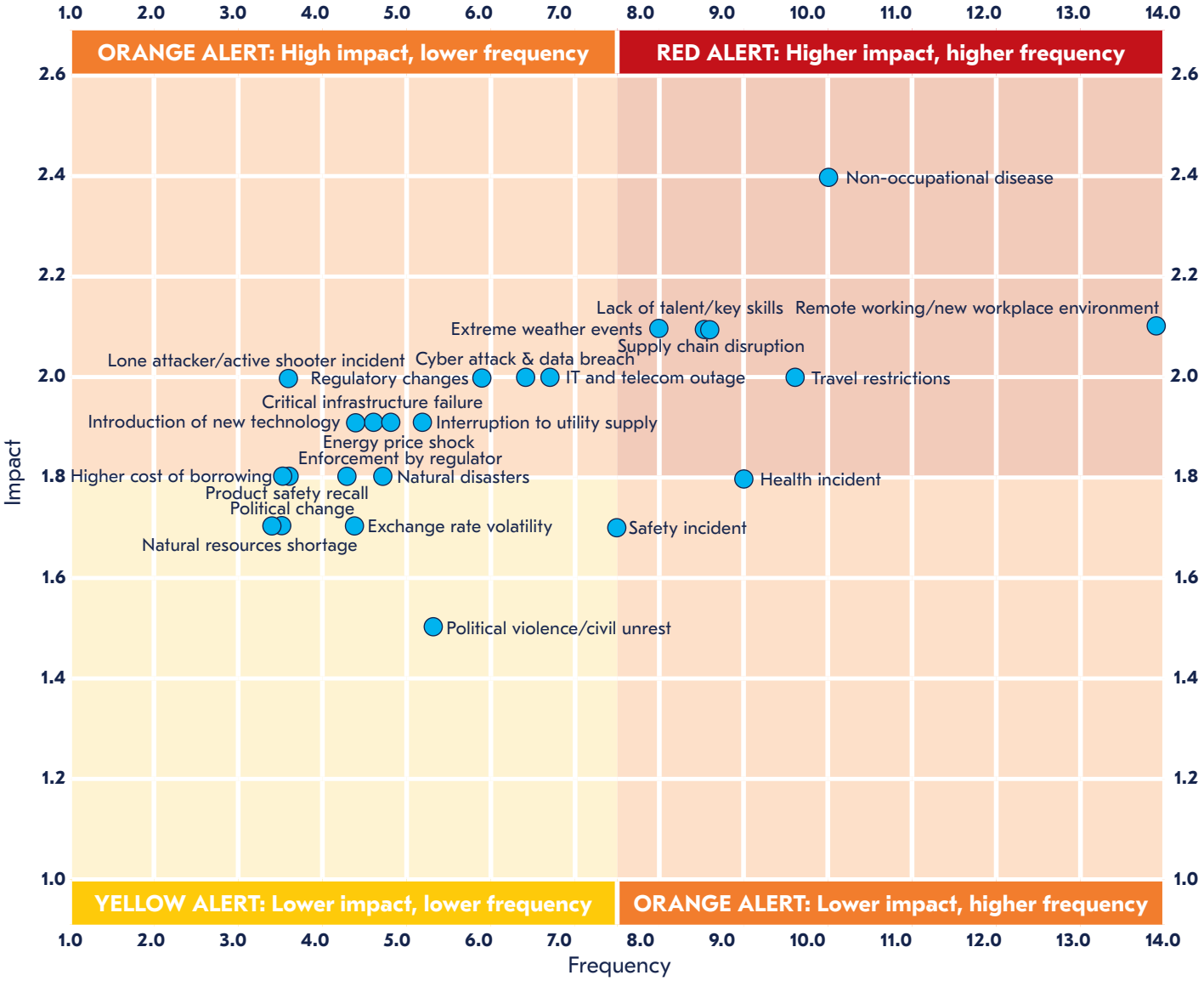


Figure 22. Risk and threat assessment: past twelve months (Americas)

Asia Pacific: next twelve months

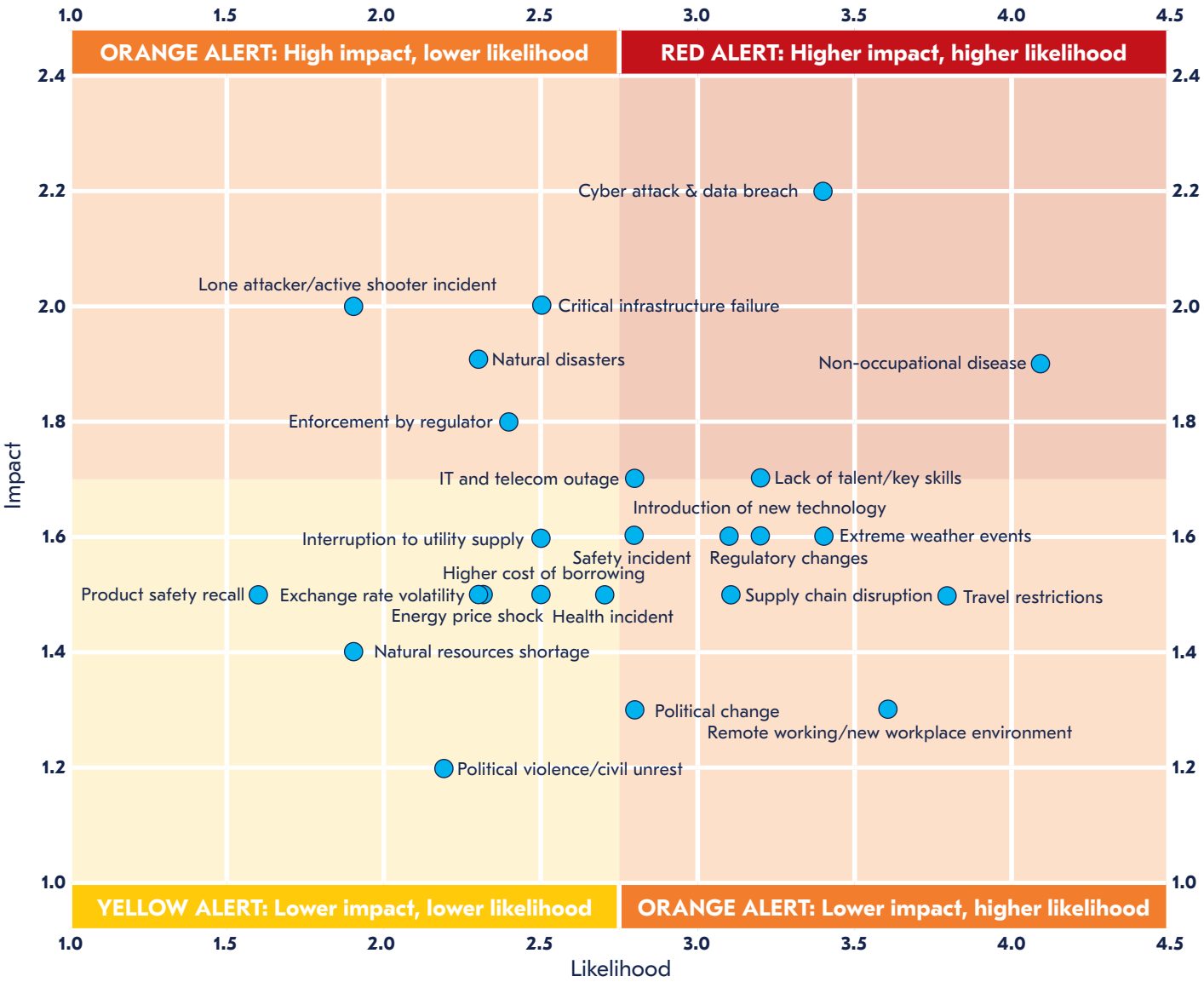


Figure 23. Risk and threat assessment: next twelve months (Asia Pacific)

Europe, Middle East and Africa: next twelve months

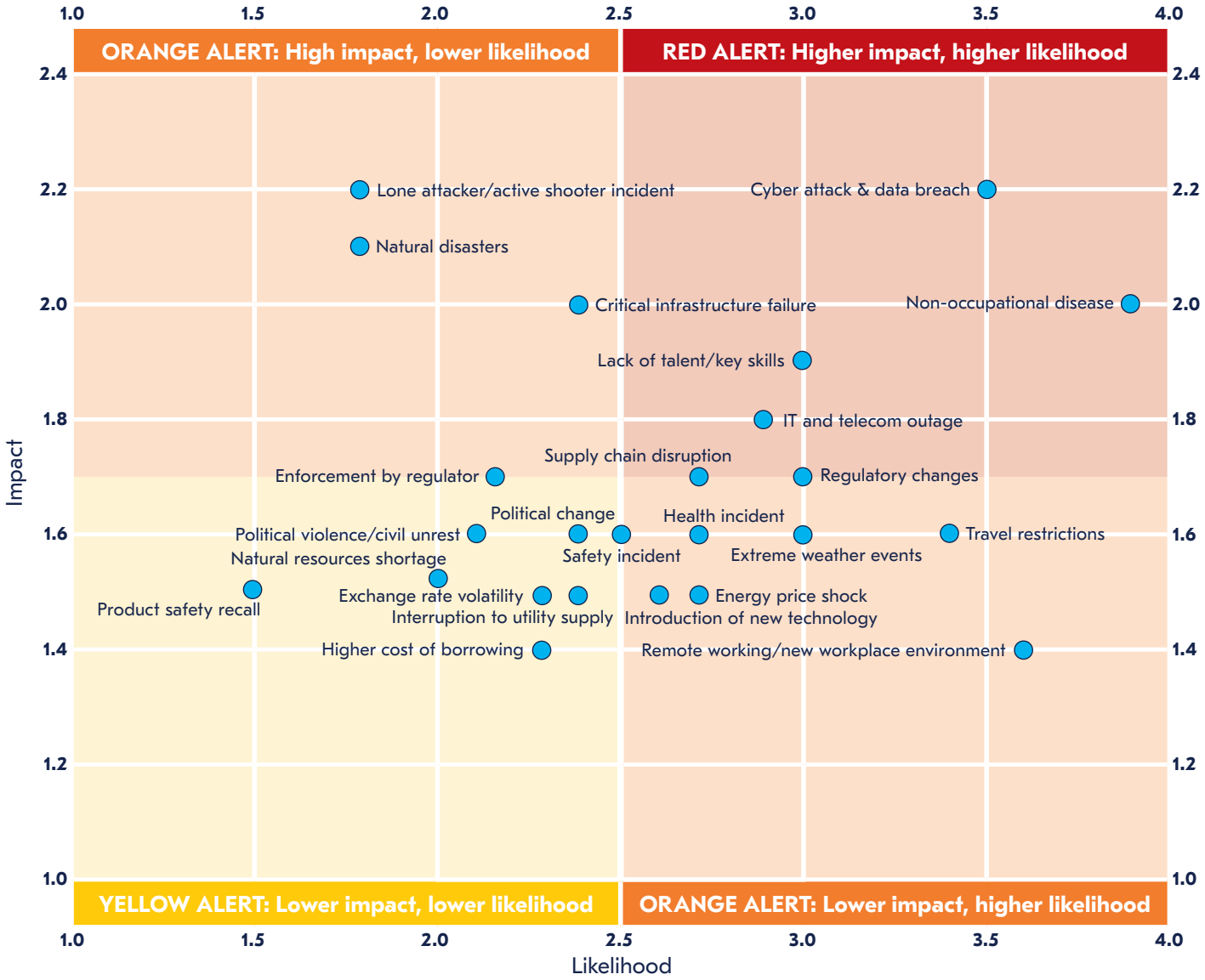


Figure 24. Risk and threat assessment: next twelve months (Europe, Middle East and Africa)

Americas: next twelve months

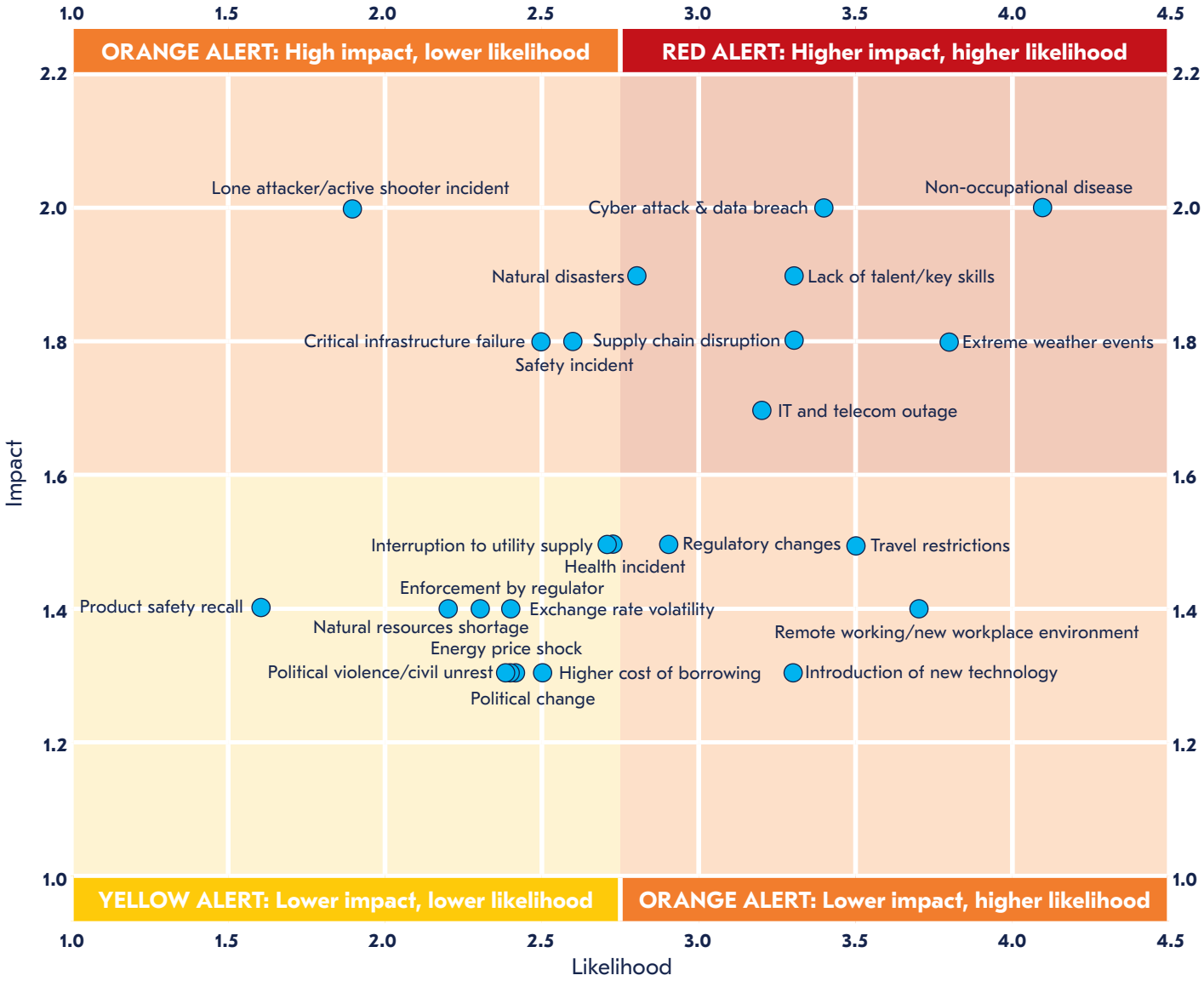


Figure 25. Risk and threat assessment: next twelve months (Americas)

About the Authors

Rachael Elliott

(Head of Thought Leadership)

Rachael has twenty years' experience leading commercial research within organizations such as HSBC, BDO LLP, Marakon Associates, CBRE and BCMS. She has particular expertise in the technology & telecoms, retail, manufacturing and real estate sectors. Her research has been used in Parliament to help develop government industrial strategy and the BDO High Street Sales Tracker, which Rachael was instrumental in developing, is still the UK's primary barometer for tracking high street sales performance. She maintains a keen interest in competitive intelligence and investigative research techniques.

She can be contacted at rachael.elliott@thebci.org

Gianluca Riglietti

(Content Specialist in Business Continuity and Resilience)

Gianluca is a researcher and a freelance content creator interested in the development of resilient and safe societies. He has experience managing international research projects for companies such as BSI, Zurich, Everbridge and SAP. He works regularly with a number of organizations in the field of organizational resilience, such as the Business Continuity Institute. In his publications he has addressed a wealth of topics, such as climate change, cybersecurity, supply chain management and business continuity. He is also a PhD Candidate at Politecnico di Milano, where he investigates the impact of business continuity management on supply chain resilience.

He can be contacted at SCWF@protonmail.com.

About the BCI

Founded in 1994 with the aim of promoting a more resilient world, the Business Continuity Institute BCI has established itself as the world's leading Institute for Business Continuity and Resilience. The BCI has become the membership and certifying organization of choice for Business Continuity and Resilience professionals globally with over 9,000 members in more than 100 countries, working in an estimated 3,000 organizations in the private, public and third sectors. The vast experience of the Institute's broad membership and partner network is built into its world class education, continuing professional development and networking activities. Every year, more than 1,500 people choose BCI training, with options ranging from short awareness raising tools to a full academic qualification, available online and in a classroom. The Institute stands for excellence in the Resilience profession and its globally recognised Certified grades provide assurance of technical and professional competency. The BCI offers a wide range of resources for professionals seeking to raise their organization's level of Resilience, and its extensive thought leadership and research programme helps drive the industry forward. With approximately 120 Partners worldwide, the BCI Partnership offers organizations the opportunity to work with the BCI in promoting best practice in Business Continuity and Resilience.

The BCI welcomes everyone with an interest in building resilient organizations from newcomers, experienced professionals and organizations. Further information about the BCI is available at **www.thebci.org**.

Contact the BCI

+44 118 947 8215 | bci@thebci.org
10-11 Southview Park, Marsack Street, Caversham, RG4 5AF, United Kingdom.

About BSI

BSI is the business improvement company that enables organizations to turn standards of best practice into habits of excellence, 'inspiring trust for a more resilient world'. For over a century BSI has driven best practice in organizations around the world. Working with 84,000 clients across 195 countries, it is a truly global business with skills and experience across all sectors including automotive, aerospace, built environment, food and retail and healthcare. Through its expertise in Standards and Knowledge Solutions, Assurance Services, Regulatory Services and Consulting Services, BSI helps clients to improve their performance, grow sustainably, manage risk and ultimately become more resilient.

Visit: bsigroup.com

Correct as of March 2022

BCI 10-11 Southview Park, Marsack Street,
Caversham, Berkshire, UK, RG4 5AF

bci@thebci.org / www.thebci.org

bsi.

bci Leading the way to resilience

WORLD ECONOMIC FORUM

The Global Risks Report 2022

17th Edition

INSIGHT REPORT

In partnership with Marsh McLennan, SK Group and Zurich Insurance Group

The Global Risks Report 2022, 17th Edition, is published by the World Economic Forum.

The information in this report, or on which this report is based, has been obtained from sources that the authors believe to be reliable and accurate. However, it has not been independently verified and no representation or warranty, express or implied, is made as to the accuracy or completeness of any information obtained from third parties. In addition, the statements in this report may provide current expectations of future events based on certain assumptions and include any statement that does not directly relate to a historical fact or a current fact. These statements involve known and unknown risks, uncertainties and other factors which are not exhaustive. The companies contributing to this report operate in a continually changing environment and new risks emerge continually. Readers are cautioned not to place undue reliance on these statements. The companies contributing to this report undertake no obligation to publicly revise or update any statements, whether as a result of new information, future events or otherwise and they shall in no event be liable for any loss or damage arising in connection with the use of the information in this report.

World Economic Forum ®

Cover artwork: SMOG

© 2022 – All rights reserved.

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, or otherwise without the prior permission of the World Economic Forum.

ISBN: 978-2-940631-09-4

The report and an interactive data platform are available at wef.ch/risks22

The Global Risks Report 2022
17th Edition

Strategic Partners
Marsh McLennan
SK Group
Zurich Insurance Group

Academic Advisers
National University of Singapore
Oxford Martin School, University of Oxford
Wharton Risk Management and Decision Processes Center, University of Pennsylvania

CONTENTS

Preface 5—6

Executive Summary 7—10

CHAPTER 1

Global Risks 2022: Worlds Apart

including Global Risks Perception Survey 2021–2022 Results 11—29

CHAPTER 2

Disorderly Climate Transition 30—44

CHAPTER 3

Digital Dependencies and Cyber Vulnerabilities 45—56

CHAPTER 4

Barriers to Migration 57—69

CHAPTER 5

Crowding and Competition in Space 70—79

CHAPTER 6

Refreshing Resilience 80—91

Appendices

Appendix A: Description of Global Risks 2022

Appendix B: Executive Opinion Survey National Risk Perceptions

Appendix C: Technical Notes: Global Risks Perception Survey 2021–2022 92—112

Acknowledgements 113—116

Preface

By **Klaus Schwab** and **Børge Brende**

A divergent economic recovery from the crisis created by the pandemic risks deepening global divisions at a time when societies and the international community urgently need to collaborate to check COVID-19, heal its scars and address compounding global risks.

In some societies, rapid progress on vaccination, leaps forward on digitalization and a return to pre-pandemic growth rates herald better prospects for 2022 and beyond. Others could be weighed down for years by struggles to apply even initial vaccine doses, combat digital divides and find new sources of economic growth. Widening disparities within and between countries will not only make it more difficult to control COVID-19 and its variants, but will also risk stalling, if not reversing, joint action against shared threats that the world cannot afford to overlook.

Last year's edition of the *Global Risks Report* warned of potential knock-on economic risks that are now clear and present dangers. Supply chain disruptions, inflation, debt, labour market gaps, protectionism and educational disparities are moving the world economy into choppy waters that both rapidly and slowly recovering countries alike will need to navigate to restore social cohesion, boost employment and thrive. These difficulties are impeding the visibility of emerging challenges, which include climate transition disorder, increased cyber vulnerabilities, greater barriers to international mobility, and crowding and competition in space.

Restoring trust and fostering cooperation within and between countries will be crucial to addressing these challenges and preventing the world from drifting further apart.

The 17th edition of the *Global Risks Report* identifies tensions that will result from diverging trajectories and approaches within and between countries and then examines the risks that could arise from such tensions. This year's report also highlights the implications of these risks for individuals, governments and businesses.

The Global Risks Perception Survey (GRPS), which has underpinned the report since 2006, was refreshed this year to gather new and broader insights from nearly 1,000 global experts and leaders who responded. The 2021-2022 GRPS includes the following sections:

- **COVID-19 Hindsight** invites respondents to opine on the reverberations of the crisis, allowing comparability with the results from the previous year.
- **Future Outlook** captures respondent sentiment, informing our analysis of how individual contexts may influence global risk perceptions andaffect mitigation.
- **Horizon** captures respondents' perceived trajectory and sense of urgency of global risks, informing our analysis of choices and trade-offs that decision-makers may face.
- **Severity** ranks potential damage while **Effects** asks respondents to consider cascading impacts in conjunction with the severity of the risk itself.
- **International Mitigation** asks respondents to assess international efforts in 15 global governance areas to identify achievements and areas of opportunity for global action and cooperation.
- **Open questions on risks, trends and warning signs** source expert knowledge.

This year the *Global Risks Report* also draws on the views of over 12,000 country-level leaders who identified critical short-term risks to their 124 countries, gathered through the World Economic Forum's Executive Opinion Survey. The areas highlighted in these responses are likely to inform national decision-making and provide a perspective on how short-term risk national priorities may compare with global risks and perspectives.

We are ever grateful to our partners in the report's development: Marsh McLennan, SK Group and Zurich Insurance Group. We also thank our academic partners: the National University of Singapore, the Oxford Martin School at the University of Oxford and the Wharton Risk Management and Decision Processes Center at the University of Pennsylvania.

This report continues to leverage the collective intelligence of an expanding community of the world's foremost risk experts, convened by the World Economic Forum's Global Risks Practice: the Global Risks Report Advisory Board, the Chief Risk Officers Community and the Global Future Council on Frontier Risks, as well as a series of consultations with regional and thematic experts from the public and private sectors.

The report also draws from and supports the World Economic Forum's platforms dedicated to catalysing a new economy and society, accelerating climate action for people and planet, leveraging Fourth Industrial Revolution technologies, stewarding industry transformations and enhancing global and regional cooperation. These platforms and their stakeholders use the insights from this report to shape their agendas for tackling the world's greatest challenges and embedding greater resilience and cooperation.

Executive Summary

As 2022 begins, COVID-19 and its economic and societal consequences continue to pose a critical threat to the world. Vaccine inequality and a resultant uneven economic recovery risk compounding social fractures and geopolitical tensions. In the poorest 52 countries—home to 20% of the world's people—only 6% of the population had been vaccinated at the time of writing. By 2024, developing economies (excluding China) will have fallen 5.5% below their pre-pandemic expected GDP growth, while advanced economies will have surpassed it by 0.9%—widening the global income gap.

The resulting global divergence will create tensions—within and across borders—that risk worsening the pandemic's cascading impacts and complicating the coordination needed to tackle common challenges including strengthening climate action, enhancing digital safety, restoring livelihoods and societal cohesion and managing competition in space.

The *Global Risks Report 2022* presents the results of the latest Global Risks Perception Survey (GRPS), followed by an analysis of key risks emanating from current economic, societal, environmental and technological tensions. The report concludes with reflections on enhancing resilience, drawing from the lessons of the last two years of the COVID-19 pandemic. The key findings of the survey and the analysis are summarized below.

Global risks perceptions highlight societal and environmental concerns

Asked to take a view of the past two years, respondents to the GRPS perceive societal risks—in the form of "social cohesion erosion", "livelihood crises" and "mental health deterioration"—as those that have worsened the most since the pandemic began. Only 16% of respondents feel positive and optimistic about the outlook for the world, and just 11% believe the global recovery will accelerate. Most respondents instead expect the next three years to be characterized by either consistent volatility and multiple surprises or fractured trajectories that will separate relative winners and losers.

For the next five years, respondents again signal societal and environmental risks as the most concerning. However, over a 10-year horizon, the health of the planet dominates concerns: environmental risks are perceived to be the five most critical long-term threats to the world as well as the most potentially damaging to people and planet, with "climate action failure", "extreme weather", and "biodiversity loss" ranking as the top three most severe risks. Respondents also signalled "debt crises" and "geoeconomic confrontations" as among the most severe risks over the next 10 years.

Technological risks—such as "digital inequality" and "cybersecurity failure"—are other critical short- and medium-term threats to the world according to GRPS respondents, but these fall back in the rankings towards the long term and none appear among the most potentially severe, signalling a possible blind spot in risk perceptions.

The 2021-2022 GRPS included a question on international risk mitigation efforts. "Artificial intelligence", "space exploitation", "cross-border cyberattacks and misinformation" and "migration and refugees" are the areas where most respondents believe the current state of risk mitigation efforts fall short of the challenge—that is, efforts are "not started" or in "early development". Meanwhile, for "trade facilitation", "international crime" and "weapons of mass destruction", large majorities perceived risk mitigation efforts to be "established" or "effective".

REUTERS/HEO RAN

A divergent economic recovery threatens collaboration on global challenges

Economic challenges flowing from the pandemic persist. The outlook remains weak: at the time of writing, the global economy was expected to be 2.3% smaller by 2024 than it would have been without the pandemic. Rising commodity prices, inflation and debt are emerging risks. Moreover, with another spike in COVID-19 cases towards the end of 2021, the pandemic continues to stifle countries' ability to facilitate a sustained recovery.

The economic fallout from the pandemic is compounding with labour market imbalances, protectionism, and widening digital, education and skills gaps that risk splitting the world into divergent trajectories. In some countries, rapid vaccine rollout, successful digital transformations and new growth opportunities could mean a return to pre-pandemic trends in the short term and the possibility of a more resilient outlook over a longer horizon. Yet many other countries will be held back by low rates of vaccination, continued acute stress on health systems, digital divides and stagnant job markets. These divergences will complicate the international collaboration needed to address the worsening impacts of climate change, manage migration flows and combat dangerous cyber-risks.

Short-term domestic pressures will make it harder for governments to focus on long-term priorities and will limit the political capital allocated to global concerns. "Social cohesion erosion" is a top short-term threat in 31 countries—including Argentina, France, Germany, Mexico and South Africa from the G20. Disparities that were already challenging societies are now expected to widen—51 million more people are projected to live in extreme poverty compared to the pre-pandemic trend—at the risk of increasing polarization and resentment within societies. At the same time, domestic pressures risk stronger national interest postures and worsening fractures in the global economy that will come at the expense of foreign aid and cooperation.

A disorderly climate transition will exacerbate inequalities

Respondents to the GRPS rank "climate action failure" as the number one long-term threat to the world and the risk with potentially the most severe impacts over the next decade. Climate change is already manifesting rapidly in the form of droughts, fires, floods, resource scarcity and species loss, among other impacts. In 2020, multiple cities around the world experienced extreme temperatures not seen for years—such as a record high of 42.7°C in Madrid and a 72-year low of -19°C in Dallas, and regions like the Arctic Circle have averaged summer temperatures 10°C higher

than in prior years. Governments, businesses and societies are facing increasing pressure to thwart the worst consequences. Yet a disorderly climate transition characterized by divergent trajectories worldwide and across sectors will further drive apart countries and bifurcate societies, creating barriers to cooperation.

Given the complexities of technological, economic and societal change at this scale, and the insufficient nature of current commitments, it is likely that any transition that achieves the net zero goal by 2050 will be disorderly. While COVID-19 lockdowns saw a global dip in greenhouse gas (GHG) emissions, upward trajectories soon resumed: the GHG emission rate rose faster in 2020 than the average over the last decade. Countries continuing down the path of reliance on carbon-intensive sectors risk losing competitive advantage through a higher cost of carbon, reduced resilience, failure to keep up with technological innovation and limited leverage in trade agreements. Yet shifting away from carbon-intense industries, which currently employ millions of workers, will trigger economic volatility, deepen unemployment and increase societal and geopolitical tensions. Adopting hasty environmental policies will also have unintended consequences for nature—there are still many unknown risks from deploying untested biotechnical and geoengineering technologies—while lack of public support for land use transitions or new pricing schemes will create political complications that further slow action. A transition that fails to account for societal implications will exacerbate inequalities within and between countries, heightening geopolitical frictions.

Growing digital dependency will intensify cyberthreats

Growing dependency on digital systems—intensified by COVID-19—has altered societies. Over the last 18 months, industries have undergone rapid digitalization, workers have shifted to remote working where possible, and platforms and devices facilitating this change have proliferated. At the same time, cybersecurity threats are growing—in 2020, malware and ransomware attacks increased by 358% and 435% respectively—and are outpacing societies' ability to effectively prevent or respond to them. Lower barriers to entry for cyberthreat actors, more aggressive attack methods, a dearth of cybersecurity professionals and patchwork governance mechanisms are all aggravating the risk.

Attacks on large and strategic systems will carry cascading physical consequences across societies, while prevention will inevitably entail higher costs. Intangible risks—such as disinformation, fraud and lack of digital safety—will also impact public trust in digital systems. Greater cyberthreats will also hamper cooperation between states if governments continue to follow unilateral paths to control risks. As attacks become more severe and broadly impactful, already-sharp tensions between governments impacted by cybercrime and governments complicit in their commission will rise as cybersecurity becomes another wedge for divergence—rather than cooperation—among nation-states.

Barriers to mobility risk compounding global insecurity

Growing insecurity resulting from economic hardship, intensifying impacts of climate change and political instability are already forcing millions to leave their homes in search of a better future abroad. "Involuntary migration" is a top long-term concern for GRPS respondents, while 60% of them see "migration and refugees" as an area where international mitigation efforts have "not started" or are in "early development". In 2020, there were over 34 million people displaced abroad globally from conflict alone—a historical high. However, in many countries, the lingering effects of the pandemic, increased economic protectionism and new labour market dynamics are resulting in higher barriers to entry for migrants who might seek opportunity or refuge.

These higher barriers to migration, and their spill-over effect on remittances—a critical lifeline for some developing countries—risk precluding a potential pathway to restoring livelihoods, maintaining political stability and closing income and labour gaps. At the time of writing, the United States faced over 11 million unfilled jobs in general and the European Union had a deficit of 400,000 drivers just in the trucking industry. In the most extreme cases, humanitarian crises will worsen since vulnerable groups have no choice but to embark on more dangerous journeys. Migration pressures will also exacerbate international tensions as it is increasingly used as a geopolitical instrument. Destination-country governments will have to manage diplomatic relationships and immigrant skepticism among their populations.

Opportunities in space could be constrained by frictions

While humans have been exploring space for decades, recent years have witnessed increased activity, not only creating new opportunities but also signalling an emerging realm of risk, particularly with growing militarization and weaponization in the arena. New

commercial satellite market entrants are disrupting incumbents' traditional influence over the global space commons in delivering satellite services, notably internet-related communications. A greater number and range of actors operating in space could generate frictions if space exploration and exploitation are not responsibly managed. With limited and outdated global governance in place to regulate space alongside diverging national-level policies, risks are intensifying.

One consequence of accelerated space activity is a higher risk of collisions that could lead to a proliferation of space debris and impact the orbits that host infrastructure for key systems on Earth, damage valuable space equipment or spark international tensions. Limited governance tools increase the likelihood of space activity escalating geopolitical tensions, and recent weapons tests in space underscore such risks. Increased space activity could also lead to unknown environmental impacts or raise costs for public goods such as weather monitoring or climate change surveillance.

Year two of the pandemic yields insights on resilience

In 2021, countries deployed new mechanisms to respond to a public health crisis with shifting characteristics, leading to both successes and failures. Two interlinked factors were critical for effective management of the pandemic: first, the readiness of governments to adjust and modify response strategies according to changing circumstances; and second, their ability to maintain societal trust through principled decisions and effective communication.

Reflecting on the distinct resilience goals of governments, businesses and communities will help ensure that agendas are aligned in achieving a whole-of-society approach to tackling critical risks of any nature. For governments, balancing costs, regulating for resilience and adjusting data-sharing arrangements to ensure sharper crisis management are key to galvanizing stronger interaction between public and private sectors. Businesses—recognizing that better national-level preparedness is critical for planning, investing and executing their strategies—can leverage opportunities in areas such as supply chains, codes of conduct within their industry and inclusion of a resilience dimension into workforce benefit offerings. Communities can help local governments to join up with national efforts, improve communication and support grassroots resilience efforts. At an organizational level, strategies such as grounding resilience analyses in key delivery requirements, appreciating systemic vulnerabilities and embracing a diversity of approaches can help leaders build better resilience as well.

REUTERS/MUHAMMAD HAMED

CHAPTER 1

Global Risks 2022: Worlds Apart

6%

vaccination rate in poorest 52 countries

97%

public debt-to-GDP in 2020

51 million

increase in extreme poverty projections

197

countries aligned on the Glasgow Climate Pact

84%

of experts are worried or concerned about the world

GETTY/ABSTRACT AERIAL ART

A divergent recovery

At the start of 2022, the COVID-19 crisis is still ongoing and its economic ructions continue to be felt. Disparities in progress on vaccination are creating a divergent economic recovery that risks compounding pre-existing social cleavages and geopolitical tensions. These tensions and the economic overhang of the pandemic will make it difficult to ensure a coordinated and sufficiently rapid approach to global challenges—most notably climate change.

Vaccination and accelerated digitalization have enabled some countries to recover rapidly from the economic crisis created by the COVID-19 pandemic, but many others are still struggling to avoid the worst consequences. At the time of writing, half of the world's population was still unvaccinated,[1] 40% remained offline,[2] and only 35% of the world's students lived in countries where schools are fully open.[3] Some 37% of respondents to this year's Global Risks Perceptions Survey (GRPS) believe the world will follow a fractured trajectory in the medium term, increasingly separating relative "winners" from "losers" of the COVID-19 crisis (see Figure 1.1). By the time the GRPS was conducted (see the Technical Notes in Appendix C), only 11% believed the global recovery would accelerate over the next three years.

Economic, geopolitical, public health and societal fractures—which increase after pandemics[4]—risk leading to divergent and delayed approaches to critical challenges facing people and planet: accelerating the green transition in response to climate change (see Chapter 2), coordinating against heightened digital vulnerabilities (see Chapter 3), managing mobility and migration (see Chapter 4) and safeguarding the next global commons: space (see Chapter 5).

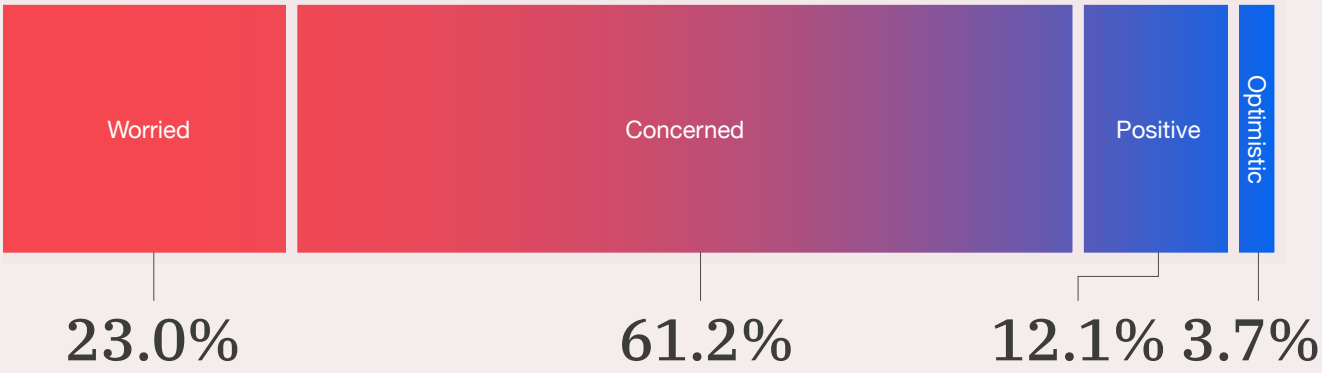
FIGURE 1.1

"What is your outlook for the world over the next three years?"

Source: World Economic Forum Global Risks Perception Survey 2021-2022

FIGURE 1.2

"How do you feel about the outlook for the world?"



Source: World Economic Forum Global Risks Perception Survey 2021-2022

Effective domestic and international action on these challenges depends on restoring trust within societies, galvanizing national and global leaders and finding new opportunities for collaboration (see Chapter 6). Fully 84% of GRPS respondents were either concerned or worried about the outlook for the world (see Figure 1.2); lack of optimism could create a vicious cycle of disillusionment and social unrest.

A turbulent global context

The pandemic persists

The world continues to grapple with the effects of COVID-19 on public health. At the start of 2022, 5.4 million deaths from COVID-19 had been reported globally, out of 282 million confirmed cases.[5] Moreover, a significant proportion of those infected by COVID-19 have long-lasting symptoms—some 10% show persistent ill health 12 weeks after having the disease.[6] COVID-19 vaccination has progressed steadily but unevenly around the world. At the time of writing, 50 countries had vaccinated more than 70% of their population,[7] with some now starting to receive booster shots, while the vaccination rate in the poorest 52 countries—home to 20% of the world's population—was still only 6%.[8] Potentially more infectious variants of the virus—notably the new Omicron variant—along with waning immunity among the vaccinated and a continued high proportion of people who are unvaccinated meant that the number of new cases increased again towards the end of 2021.[9] Unsurprisingly, "infectious diseases" are still considered a critical short-term threat to the world in the GRPS.

The COVID-19 crisis has also had extensive collateral health impacts, partly because other diseases were deprioritized. The pandemic led to an additional 53 million cases of major depression globally.[10] "Mental health deterioration" was one of the top five risks that GRPS respondents saw as having deteriorated the most during COVID-19. The incidence of non-communicable diseases—which cause 41 million deaths every year, mostly in low- and middle-income countries—has also worsened worldwide due to treatment delays caused by COVID-19.[11] Antimicrobial resistance caused nearly 2 million deaths in 2020 and this number may increase—particularly for malaria and tuberculosis—because of the inappropriate use of antibiotics to treat COVID-19.[12] The pandemic and its collateral health impacts

will continue to put pressure on health systems across the globe, widen health inequalities between and within countries, create social frictions and weigh down long-term economic growth potential.

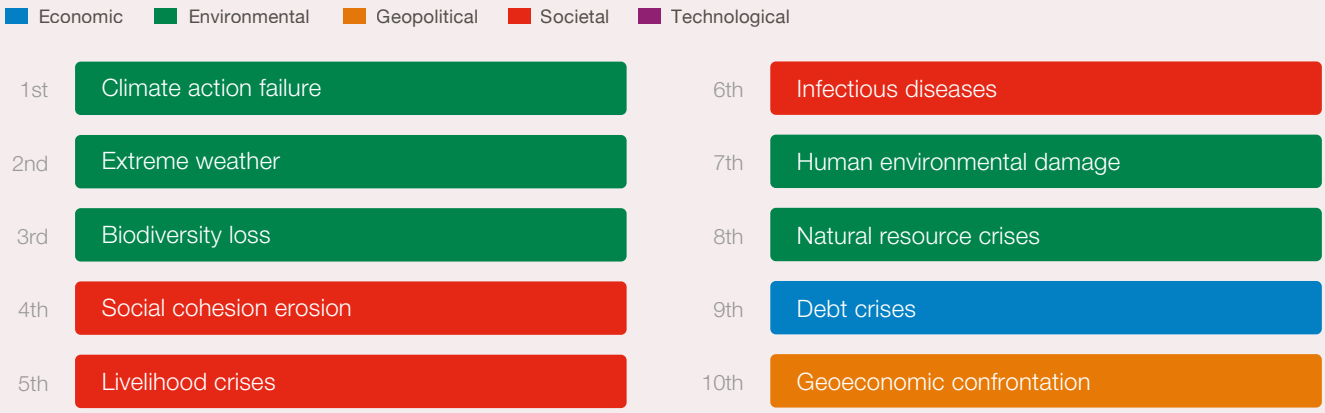
Risks to economic recovery

The global economic recovery from the recession caused by responses to the COVID-19 pandemic continues but is slowing. After a contraction of 3.1% in 2020, global economic growth is expected to reach 5.9% in 2021 and slow to 4.9% in 2022.[13] By 2024, the global economy is projected to be 2.3% smaller than it would have been without the pandemic.[14] Risks to economic growth are considerable, including risks from a potential resurgence of COVID-19 as new variants emerge. The previous edition of the GRPS identified "commodity shocks", "price instability" and "debt crises" as critical medium-term concerns. These are already emerging to some extent. At the time of writing, commodity prices had increased nearly 30% since end of 2020;[15] they could remain volatile because of growing tensions between Europe and Russia, China's energy shortage,[16] continued supply chain disruptions and transition challenges from disinvestment in fossil fuel reserves. Inflation has accelerated in many countries as a result of pandemic-related disruptions to supply chains combined with resurgent consumer demand and higher commodity prices. This will dampen consumer sentiment—which has been fundamental for recovery—and will increase risks from central bank interest rate rises.[17] In advanced and developing economies alike, higher prices and more expensive debt would impact lower-income households especially hard, while small and medium-sized enterprises (SMEs) that are still trying to avoid bankruptcy would suffer from weakening consumption.

Moreover, sovereign debt has spiked because of the pandemic. Government debt globally increased by 13 percentage points, to 97% of GDP, in 2020.[18] Already-strained public finances in developing countries are at heightened risk from debt deleveraging[19] and an appreciation of the US dollar—the US Dollar Index had risen 7% since the start of 2021.[20] GRPS respondents identified "debt crises" as a critical short- and medium-term threat to the world, and one of the most potentially severe risks over the next decade (see Figure 1.3). Debt overhangs will make it more difficult for countries to deal with the economic impacts of COVID-19 and finance a socially just, net zero transition.

FIGURE 1.3

"Identify the most severe risks on a global scale over the next 10 years"



Source: World Economic Forum Global Risks Perception Survey 2021-2022

GETTY/LIU JIN

Economic divergence

COVID-19 prompted a global recession, but stark differences in vaccination rates between countries now risk leading to even greater economic divergence than they experienced before the pandemic. A greater prevalence of COVID-19 in low-vaccination countries than in high-vaccination ones will weigh on worker availability and productivity, disrupt supply chains and weaken consumption. Moreover, a lower post-pandemic risk appetite in the vaccinated world—comprised mostly of advanced economies—could weaken their investment in the non-vaccinated world. The economic disruption from the pandemic has also created stronger incentives in the vaccinated world to prioritize resilience over cost minimization. Governments and industries may now drive regional convergence at the expense of global integration as they seek to minimize supply chain disruptions.

Polarized connectivity, education and income trajectories risk further fragmenting the global economy, and divergence is likely to be aggravated by slowing and disparate growth. Advanced economies are expected to surpass their pre-pandemic growth path by 0.9% by 2024, but developing economies (excluding China) will be 5.5% below it—with Latin America and Sub-Saharan Africa trailing even further behind.[21] Economic decoupling risks further hindering already-limited means to restore growth in developing economies. Such decoupling will make it harder for emerging economies to leverage young workforces, large consumer markets and competitive costs. They also risk having less access to financing and technology to face global challenges, including climate change.

Although employment is approaching pre-pandemic levels in many advanced economies, globally the jobs recovery from the COVID-19 crisis is lagging the economic recovery—global employment remains lower than it was before the pandemic and the Great Resignation in advanced economies has caused labour market

Income disparities risk increasing polarization and resentment within societies

participation to fall. Youth, women and lower-skilled workers have been especially affected. It will take the global economy at least until 2023 to create the jobs lost to COVID-19, but many of these jobs are expected to be of low productivity and poor quality, according to the International Labour Organization.[22] "Livelihood crises" is the second most immediate threat to the world in the GRPS, and the top one at the country level in the Executive Opinion Survey (EOS). It is the most immediate national threat in 97 countries, including 16 of the G20 economies.

A bifurcated economic recovery is likely to prompt an upsurge in economic migration. At the same time, worsening extreme weather and a rise in political instability, state fragility and civil conflict are likely to further swell refugee numbers. GRPS respondents rate "involuntary migration" as a critical threat to the world over the next decade. Yet, it is a top-10 concern in only 13 countries surveyed by the EOS—among them Armenia, El Salvador, Guatemala, Honduras, Nicaragua, Ukraine and Venezuela, which have recently experienced challenges related to migration and refugees. These results suggest that migration is perceived as a short-term challenge localized in certain countries, but a global risk in the longer term. However, the clash between heightened migration pressures in origin countries and increasing barriers to migration in destination countries risks creating tensions internationally and, in the worst cases, humanitarian crises.

Erosion of social cohesion

"Social cohesion erosion" is the risk that has worsened the most globally since the start of the COVID-19 crisis, according to the GRPS. It is perceived as a critical threat to the world across all time spans—short, medium and long term—and is seen as among the most potentially damaging for the next 10 years. In 31 out of the 124 countries surveyed in the EOS—including Argentina, France, Germany, Mexico and South Africa among the G20—"social cohesion erosion" was seen as a top-10 short-term threat to their countries. Inequality—economic, political, technological and intergenerational—was already challenging societies even before income disparities increased through the pandemic.[23] These disparities are now expected to widen further: research by the World Bank estimates that the richest 20% of the world's population will have recovered half their losses in 2021, while the poorest 20% will have lost 5% more of their income.[24] By 2030, 51 million more people are projected to live in extreme poverty compared to the pre-pandemic trend.[25] Income disparities exacerbated by an uneven economic recovery risk increasing polarization and resentment within societies.

GETTY/STR

Differing views over vaccinations and COVID-related restrictions are also adding to social pressures, with a number of countries, including in Europe, seeing riots by those opposed to government's COVID responses. Racial justice also remains a pressing issue in many countries, notably the United States.

A recent poll in the United States, for example, found "division in the country" to be voters' top concern: they expected it to worsen in 2022.[26] In Europe, another recent poll revealed significant generational differences, with 65% of respondents over 60 saying that they were "not impacted at all" by the pandemic, compared with just 43% of respondents under 30.[27] The attack on the US Capitol in January 2021 was one manifestation of the instability that political polarization risks creating.

Notwithstanding the agreements made at COP26 signal international commitment to climate action (see Box 1.1), short-term domestic pressures will make it harder for governments to focus on long-term national priorities and will limit the attention and political capital that some governments worldwide will be able or willing to allocate to global concerns. Such pressures could also lead to stronger national interest postures, which would worsen fractures in the global economy, potentially coming at the expense of foreign aid and cooperation needed to resolve conflicts, protect refugees and address humanitarian emergencies. The UK government, for instance, already dropped its target of spending 0.7% of gross national income on foreign aid until at least 2024.[28] Fragile economies could spiral into deeper crises.

Geopolitical tensions

Widening geopolitical fractures risk being another force for global divergence. Competition between the United States and China is increasing. China's growing military prowess is changing the balance of power in the Western Pacific.[29] The United States is strengthening alliances focused on the Pacific in response, most recently with the Australia-UK-US security pact

Countries may drive regional convergence at the expense of global integration

(AUKUS). Other states, such as Russia and Turkey, are also showing greater capability and willingness to project power abroad. Meanwhile, key global and regional powers are testing boundaries of international law and cooperation by conducting military exercises around tense areas, such as the Russia-Ukraine border and the Taiwan Strait. Competition is intensifying in newer dimensions and geographies, as evident in the militarization and weaponization of space (see Chapter 5) and in developments in cyberspace, where already-sharp tensions between governments impacted by cybercrime and governments complicit in their commission will continue to rise (see Chapter 3).

Competition is also increasing in the exercise of "soft power". For example, China's vaccine diplomacy, external financing strategy and economic rebound—its economy is expected to have grown by 8% annually in 2021[30]—have allowed it to continue to expand its influence throughout the developing world. Brazil, Indonesia, Mexico and Turkey are among the top buyers of Chinese COVID-19 vaccines,[31] and net debt payments to China rose by 62% in 2020.[32] Developing countries may increasingly look to China for financial, technological and scientific support to thrive in the post-pandemic economy.

Geopolitical tensions are spilling over into the economic sphere. For example, India and Japan put protectionist policies in place during the pandemic.[33] Western companies in sensitive sectors such as technology are encountering increasing difficulties in doing business in China and Russia, and Western countries are themselves restricting investment from geopolitical competitors in strategic sectors. GRPS respondents identified "geoeconomic confrontations" as a critical medium- and long-term threat

to the world, and the most potentially severe geopolitical risk for the next decade (see Figure 1.3). Geopolitical and geoeconomic tensions will make it more difficult to tackle common global challenges, notably climate change.

Risk of climate action failure

The 2021 United Nations Climate Change Conference (COP26) succeeded in getting 197 countries to align on the Glasgow Climate Pact and other landmark pledges (see Box 1.1), but even these new commitments are expected to miss the 1.5°C goal established in the 2016 Paris Climate Agreement and increase the risks from a disorderly climate transition (see Chapter 2).[34]

The economic overhang of the COVID-19 crisis and weakened social cohesion—in advanced and developing economies alike—may further limit the financial and political capital available for stronger climate action. The European Union, the United Kingdom and the United States, for example, were reluctant to commit to a formal climate finance target to respond to worsening climate change impacts in developing country Parties.[35] China and India lobbied to change the Pact's wording from "phase out" to "phase down" of "unabated coal power and inefficient fossil fuel subsidies".[36]

The economic crisis created by the COVID-19 pandemic risks delaying efforts to tackle climate change by encouraging countries to prioritize short-term measures to restore economic growth, regardless of their impact on the climate, over pursuing green transitions. Brazil, for example, joined the other 140 countries responsible for 91% of the Earth's forests in endorsing the Glasgow Leaders' Declaration on Forests and Land Use,[37] even as deforestation in the Amazon accelerated to a 15-year high in 2021 following the pandemic-induced recession of 2020.[38] Geopolitical tensions and nation-first postures will also complicate climate action. COP26 revealed heightened tensions on climate damage compensation, with affected countries facing pushback from large emitters, including the United States.[39]

Climate change continues to be perceived as the gravest threat to humanity. GRPS respondents rate "climate action failure" as the risk with potential to inflict the most damage at a global scale over the next decade (see Figure 1.3). However, EOS results hint at divergent senses of urgency between regions and countries. "Climate action failure" ranks 2nd as a short-term risk in the United States but 23rd in China—the two countries that are the world's largest CO_2 emitters. In addition to its 2nd place rank in the United States, it ranks among the top 10 short-term risks in 11 other G20 economies.

REUTERS/HANNIBAL HANSCHKE

BOX 1.1

Outcomes of COP26 and COP15

The 2021 United Nations Climate Change Conference (COP26, held in Glasgow, the United Kingdom), which passed the Glasgow Climate Pact,[1] concluded with important steps towards the 1.5°C scenario: it requested governments from 153 countries to update and strengthen their nationally determined contributions (NDCs), bolstered climate adaptation finance efforts, and continued the mobilization of billions of US dollars for climate funding and trillions to be reallocated by private institutions and central banks towards global net zero. COP26 was the first with financial sector attendance, represented by the Global Financial Alliance for Net Zero (GFANZ), whose members manage over US$130 trillion in assets and already actively fund sustainable investments.[2]

For the first time, the Pact made explicit mention of the importance of transitioning away from coal—but did not commit to "phase out" inefficient fossil fuel subsidies. However, as the United Nations Environment Programme (UNEP)'s Emissions Gap Report 2021 shows, reaching the 1.5°C target remains unlikely.[3]

Another key outcome was an agreement on the fundamental norms related to Article 6 of the Paris Agreement (on carbon markets), making it now fully operational.[4] Businesses and governments also agreed on more aggressive investment in clean technologies,[5] including a faster transition to electric vehicles and landmark pledges on methane emissions and deforestation.[6]

Key pledges achieved at COP26:

- India pledged to reach net zero emissions by 2070 and announced a target of 50% renewable energy by 2030. All the largest emitters have now agreed to start phasing out fossil fuels.
- 46 countries pledged to transition from coal to clean power by 2040.
- 104 countries pledged to a 30% cut in methane emissions by 2030. Methane accounts for 30% of historical global warming.
- 141 countries that account for 91% of the world's forests pledged to end deforestation by 2030.

The 2021 Conference of the Parties for the Convention on Biological Diversity (COP15, held in Kunming, China) resulted in "strong declarations for safeguarding life on Earth",[7] along with joint measures for conservation actions and addressing unsustainable production and consumption;[8] it also paved the way to negotiate a post-2020 global biodiversity framework for part two of COP15 in May 2022.[9]

Footnotes

1 UNFCCC. Decision -/CP.26, Advance unedited version. https://unfccc.int/sites/default/files/resource/cop26_auv_2f_cover_decision.pdf

2 UNEP. 2021. "Emissions Gap Report 2021. Addendum to the Emissions Gap Report 2021." Report. UNEP. 2021. https://wedocs.unep.org/bitstream/handle/20.500.11822/37350/AddEGR21.pdf

3 UN Climate Change Conference UK2021. 2021a. COP26 The Glasgow Climate Pact. November 2021. https://ukcop26.org/wp-content/uploads/2021/11/COP26-Presidency-Outcomes-The-Climate-Pact.pdf

4 UNFCC. 2021. "COP26 Reaches Consensus on Key Actions to Address Climate Change". UN Climate Press Release. 13 November 2021. https://unfccc.int/news/cop26-reaches-consensus-on-key-actions-to-address-climate-change

5 GFANZ. 2021. Glasgow Financial Alliance for Net Zero. https://www.gfanzero.com/

6 European Commission. 2021. Launch by United States, the European Union, and Partners of the Global Methane Pledge to Keep 1.5C Within Reach. European Commission. Statement. 2 November 2021. https://ec.europa.eu/commission/presscorner/detail/en/statement_21_5766 ; UN Climate Change Conference UK2021. 2021. "Glasgow Leaders' Declaration on Forest and Land Use". 2 November 2021. https://ukcop26.org/glasgow-leaders-declaration-on-forests-and-land-use/

7 WWF. 2021. WWF reaction to the adoption of the Kunming Declaration at COP15. World Wildlife Fund. 13 October 2021. https://wwf.panda.org/wwf_news/?3962441/WWF-reaction-to-the-adoption-of-the-Kunming-Declaration-at-COP15

8 IUCN. 2021. IUCN closing statement – part one of the UN Biodiversity Conference. 18 October 2021. https://www.iucn.org/news/secretariat/202110/iucn-closing-statement-part-one-un-biodiversity-conference

9 Convention on Biological Diversity. 2021. "Part one of UN Biodiversity Conference closes, sets stage for adoption of post-2020 global biodiversity framework at resumption in 2022". Press Release. 15 October 2021. https://www.cbd.int/doc/press/2021/pr-2021-10-15-cop15-en.pdf

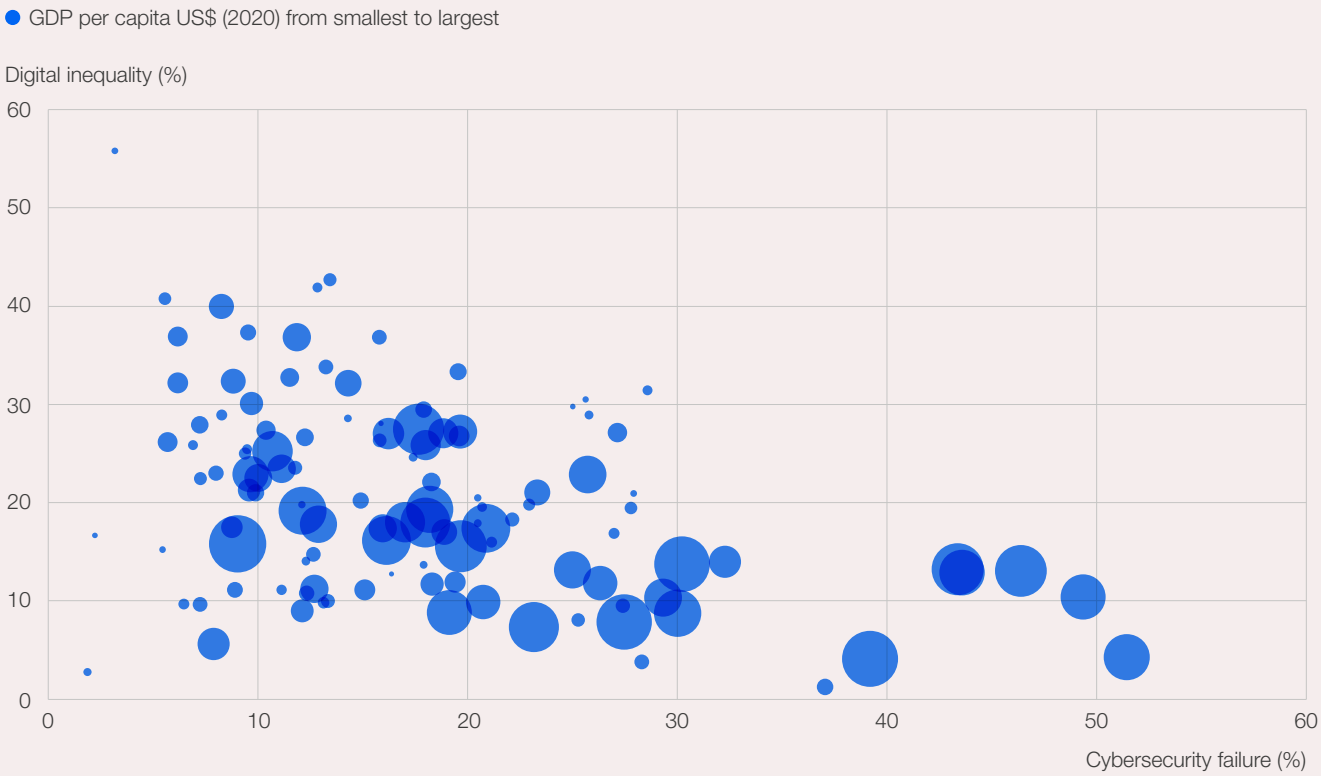
Secure digitalization

COVID-19 spurred a leap in digitalization, but to varying extents across countries. While moving towards hyperconnectivity has made some countries more competitive, others could remain stuck in a pre-pandemic analogue economy. In the latter economies, the need for rapid digitalization to avoid a widening digital divide remains pressing.[40] In the EOS, "digital inequality" is a top short-term risk in Latin America and Sub-Saharan Africa—the two regions expected to grow the least in 2022—as well as in low-income countries more widely. Governments, businesses and individuals in developing economies will be seeking to digitalize rapidly but may have limited technical and financial resources to enhance cyber defences against critical infrastructure breaches or cyber regulations to safeguard data and privacy.

More parts of the world risk becoming a base from which cybercriminals can attack globally, which could deepen digital divides if such countries then face restrictions on their access to digital technologies. Rapid digitalization in advanced economies during COVID-19 has also led to new cyber vulnerabilities. "Cybersecurity failure" was identified by GRPS respondents as a critical short-term threat to the world and scores especially high with EOS respondents in high-income countries (see Figure 1.4). There is a risk that concerns over cybersecurity could further hamper attempts to promote rapid and inclusive digitalization globally.

FIGURE 1.4

Score of "Digital Inequality" and "Cybersecurity Failure" in EOS 2021 versus GDP per Capita in 2020



Sources: World Economic Forum Executive Opinon Survey 2021; World Bank Open Data, "GDP per capita (current US$)", https://data.worldbank.org/indicator/NY.GDP.PCAP.CD, accessed 7 December 2021.

Note: Excludes Luxembourg, Switzerland and Ireland, which have the highest GDPs per capita in the EOS sample (all above US$80,000) and are distant from the rest of the sample (fourth highest is the United States, with US$63,544).

Space as a new frontier of divergence

Space is another area where global divergences risk complicating the collaboration needed to manage the development of a common good. Competition in space is rising and is a growing preoccupation for the world's leading militaries—evidenced by recent anti-satellite (ASAT) and hypersonic weapons tests.[41] Disparate economic and technological trajectories risk precluding many countries from accessing the opportunities that space entails for tackling climate change and expanding connectivity, and from ensuring that their interests are accounted for in global decision-making around space governance and commercialization. Meanwhile, increased private sector participation in space and a higher risk of congestion are creating new challenges for space governance. However, there is still time for countries to come together to ensure common benefits and sustainable management of what should be a universal resource.

Emerging tensions in global cooperation

The global divergence that risks resulting from ruptures within the world economy, stronger competition for geopolitical advantage and domestic pressures to prioritize national objectives will create complex challenges for global cooperation over the next years. Four such areas are analysed in the following deep dive chapters:

- Mounting conviction for a fast but disorderly climate transition, slowed by social, political and economic complexities, risks creating a kaleidoscope of net zero trajectories, each with different speeds and complications (see Chapter 2).
- Rapid digitalization risks exposing economies to new and more intense cyber vulnerabilities, as new technologies and an ever-expanding attack surface enable a more dangerous and diverse range of cybercrimes (see Chapter 3).
- Increased pressure for migration from origin countries as they become more insecure risks conflicting with higher barriers in destination countries (see Chapter 4).
- A new space race marked by accelerated commercial and military activity risks exacerbating tensions and oversaturation of this frontier common, highlighting the need for strengthening international governance of space (see Chapter 5).

The COVID-19 pandemic exposed the shortcomings of global cooperation, but the way forward is not clear. There is a need for stronger global governance and more effective international risk mitigation efforts, since the global, interconnected challenges highlighted in this report cannot be solved by national governments alone. Yet coming together with common purpose to achieve lasting results will be challenging: effective global governance depends on international cooperation,[42] and it will be difficult to secure traction, harness the necessary capabilities and achieve resolution on critical issues in an international relations context characterized by economic divergence, skepticism around globalization, a narrower focus on national interests and intensified geopolitical competition. Existing institutions of global governance are under pressure—as shown, for example, by the challenges that an under-resourced World Health Organization (WHO) continues to face in responding effectively to the COVID-19 pandemic.[43]

Appreciating this challenge, the final chapter of the report reflects on how governments can hedge against the prevailing limitations of multilateralism by pursuing a whole-of-society approach to bolstering national resilience (see Chapter 6).

Reflecting on the future

Crises prompt unexpected paths. Different blind spots, triggers and shocks can have a wide range of outcomes, all with varying likelihoods and impacts. As readers consider the results of the GRPS survey, review the emerging global context and read the deep dives, this report invites them to consider the behaviours and actions of specific stakeholders and to consider the consequences for a range of risk outcomes, from probable to improbable and manageable to severe.

Among the most notable areas of socio-economic concern are the divergent recovery, economic hardship and growing inequality, along with their interaction with ideological polarization and the sense of disenfranchisement of large sections of the global population. Governments' struggles to contain the pandemic and a lack of global collaboration on COVID-19 offer a sobering view of prospects for managing future global risks such as extreme weather and for pursuing bolder climate action. When it comes to business and industry, even enterprises with the financial room to manoeuvre sometimes struggle to deliver on environmental, social and governance (ESG) commitments while also strengthening the resilience of their supply chains, adapting to social and technological change and remaining vigilant to threats such as cyberattacks.

Two years on from the start of this unprecedented crisis, the actions and behaviours of all stakeholders will determine how quickly the world recovers and embeds the resilience needed to prepare for the next major shock.

REUTERS/COURTESY NXP SEMICONDUCTORS

Global Risks Perception Survey 2021-2022 Results

Scars of COVID-19

"Social cohesion erosion", "livelihood crises" and "mental health deterioration" are three of the five risks that have deteriorated the most globally through the crisis, according to the GRPS. These three risks—and the pandemic itself ("infectious diseases")—are also seen as being among the most imminent threats to the world. This societal scarring compounds the challenges of effective national policy-making and reduces the attention and focus needed on international cooperation for global challenges.

Looming debt crises

"Debt crises" were identified as an imminent threat to the world for the next two years, but GRPS respondents believe they will reach their most critical point in three to five years. Government stimulus was vital to protect incomes, preserve jobs and keep businesses afloat, but debt burdens are now high and public budgets will continue to be stretched after the pandemic, even as they are needed for financing just and green transitions.

The planet cannot wait

"Extreme weather" and "climate action failure" are among the top five short-term risks to the world, but the five most menacing long-term threats are all environmental. "Climate action failure", "extreme weather" and "biodiversity loss" also rank as the three most potentially severe risks for the next decade. While GRPS respondents' concern about environmental degradation predates the pandemic, increasing concern with climate action failure reveals respondents' lack of faith in the world's ability to contain climate change, not least because of the societal fractures and economic risks that have deepened.

Connectivity blind spots

"Digital inequality" is seen as an imminent threat to the world as 3 billion people remain offline. However, it is also the case that many countries and industries were able to quickly access and seamlessly adapt to new forms of human interaction and remote work. This digital leap came with increased vulnerability. GRPS respondents believe "cybersecurity failure" will continue to test the world's digital systems over the next two years and, to a lesser extent, in three to five years. No technological risk appears among the most potentially severe for the next decade. This suggests lower relevance to respondents—or a blind spot in perceptions given the potential damage of cyber-risks—compared to economic, societal and environmental concerns.

Growing rivalries

GRPS respondents believe "geoeconomic confrontations" will emerge as a critical threat to the world in the medium to long term and as one of the most potentially severe risks over the next decade. While pressing domestic challenges require immediate attention, the pandemic and its economic consequences have proven once again that global risks do not respect political frontiers. Humanity faces the shared and compounding threats of economic fragmentation and planetary degradation, which will require a coordinated global response.

To see the full results of the GRPS 2021-2022 see: https://www.weforum.org/reports/global-risks-report-2022/data-on-global-risks-perceptions#report-nav

FIGURE I

COVID-19 Hindsight

Risks that worsened the most since the start of the COVID-19 crisis

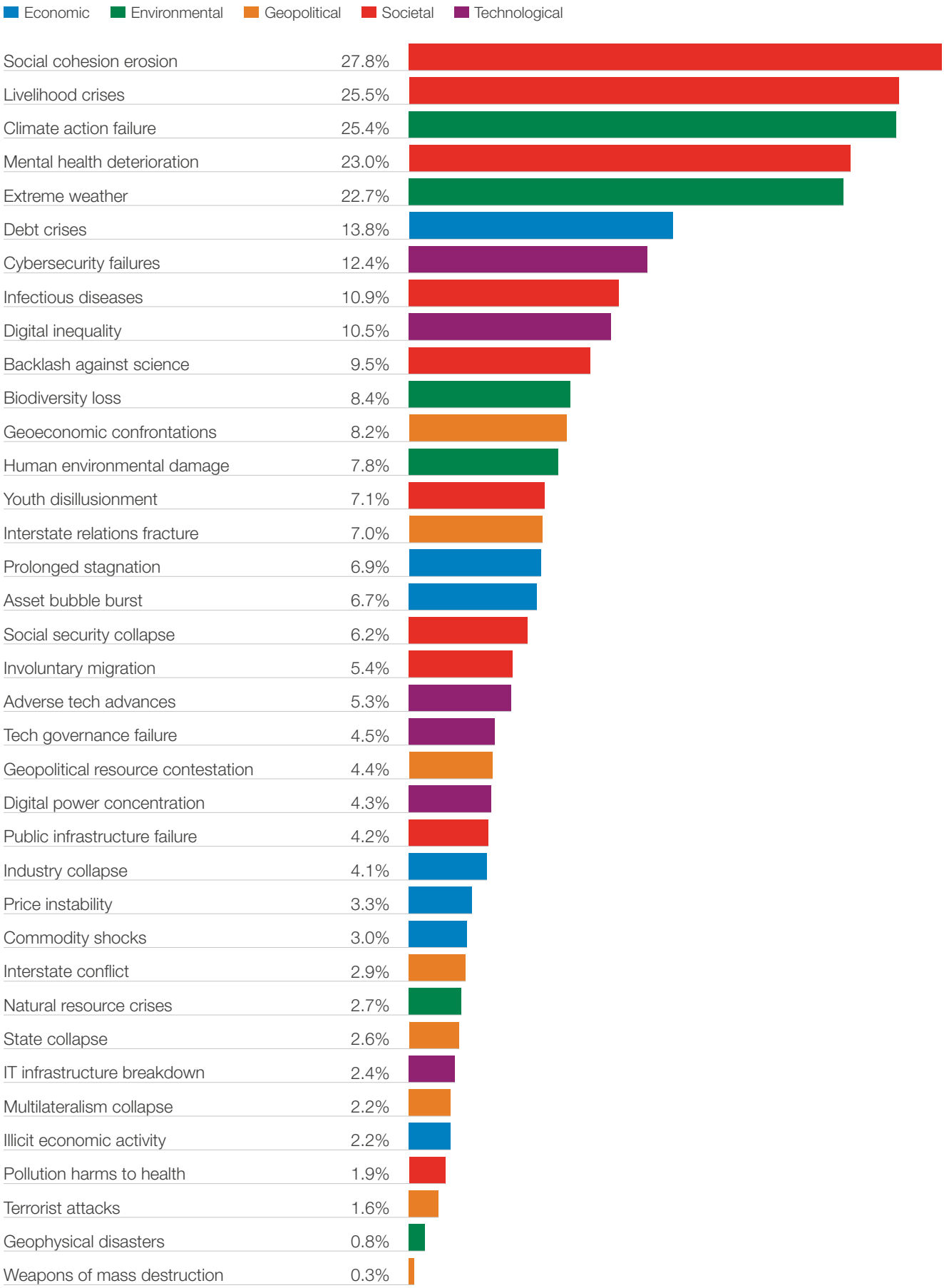


FIGURE II

Global Risks Horizon

When will risks become a critical threat to the world?

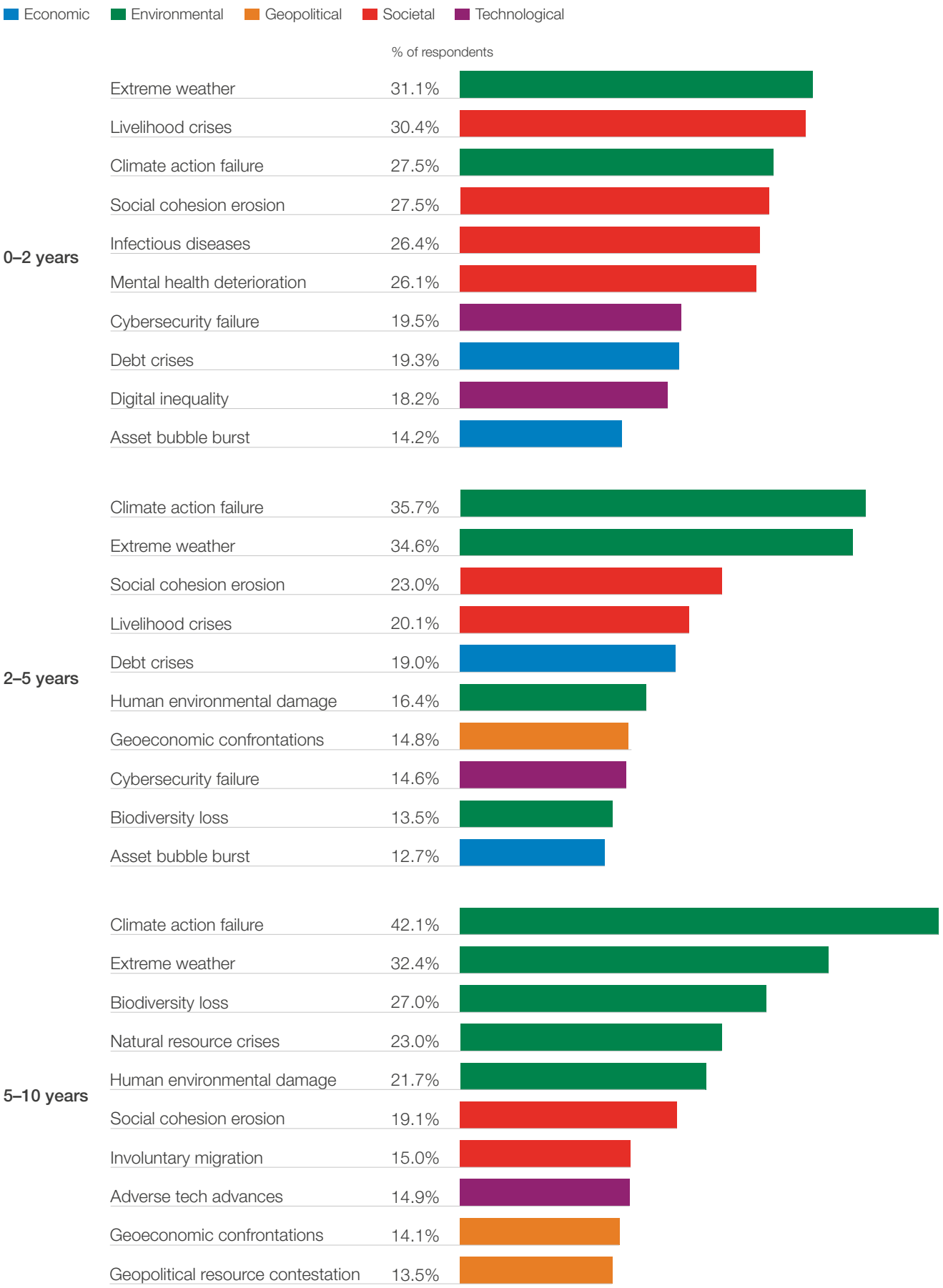
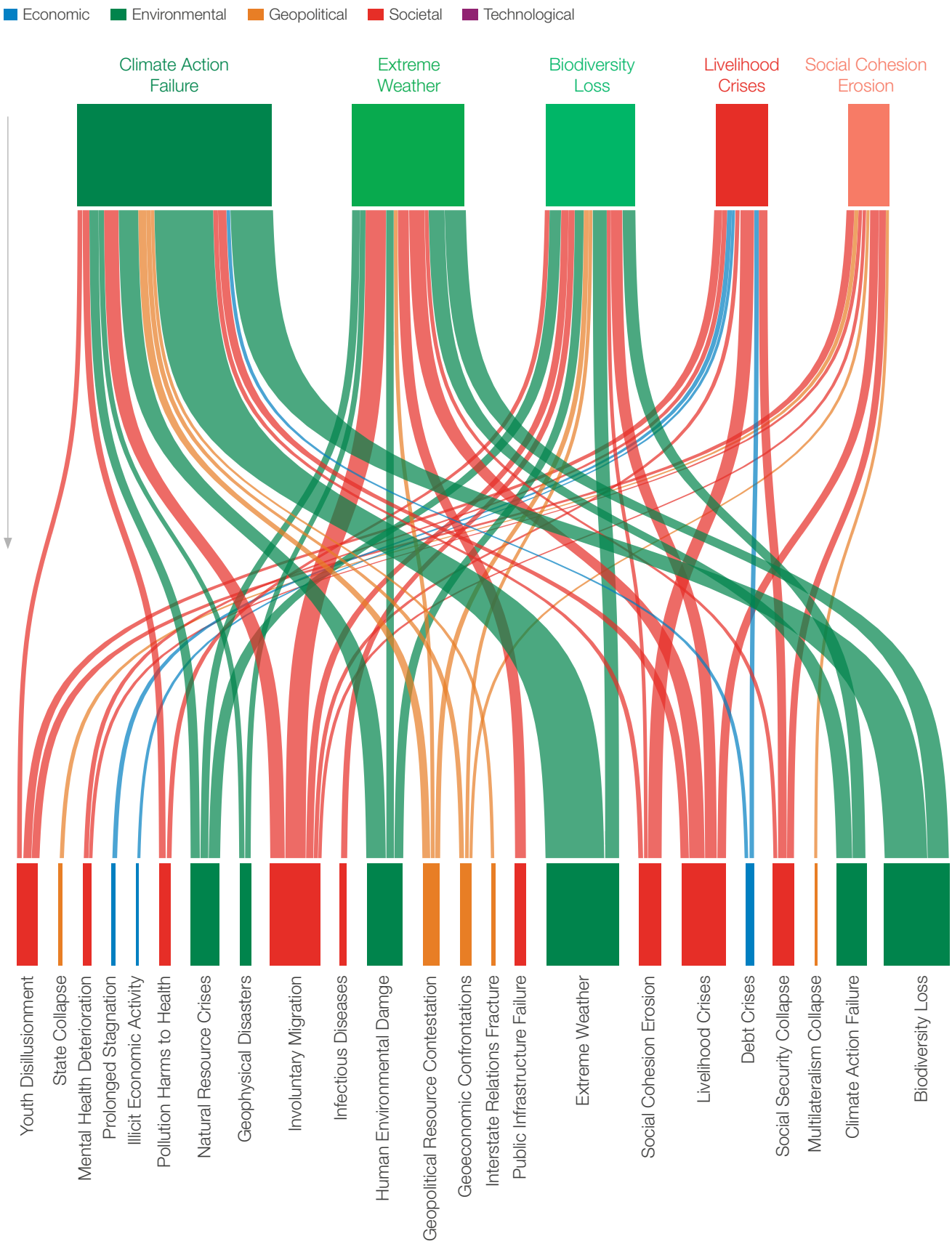


FIGURE III

Global Risks Effects

Most potentially damaging risks (top row) and risks they will aggravate (bottom row)*

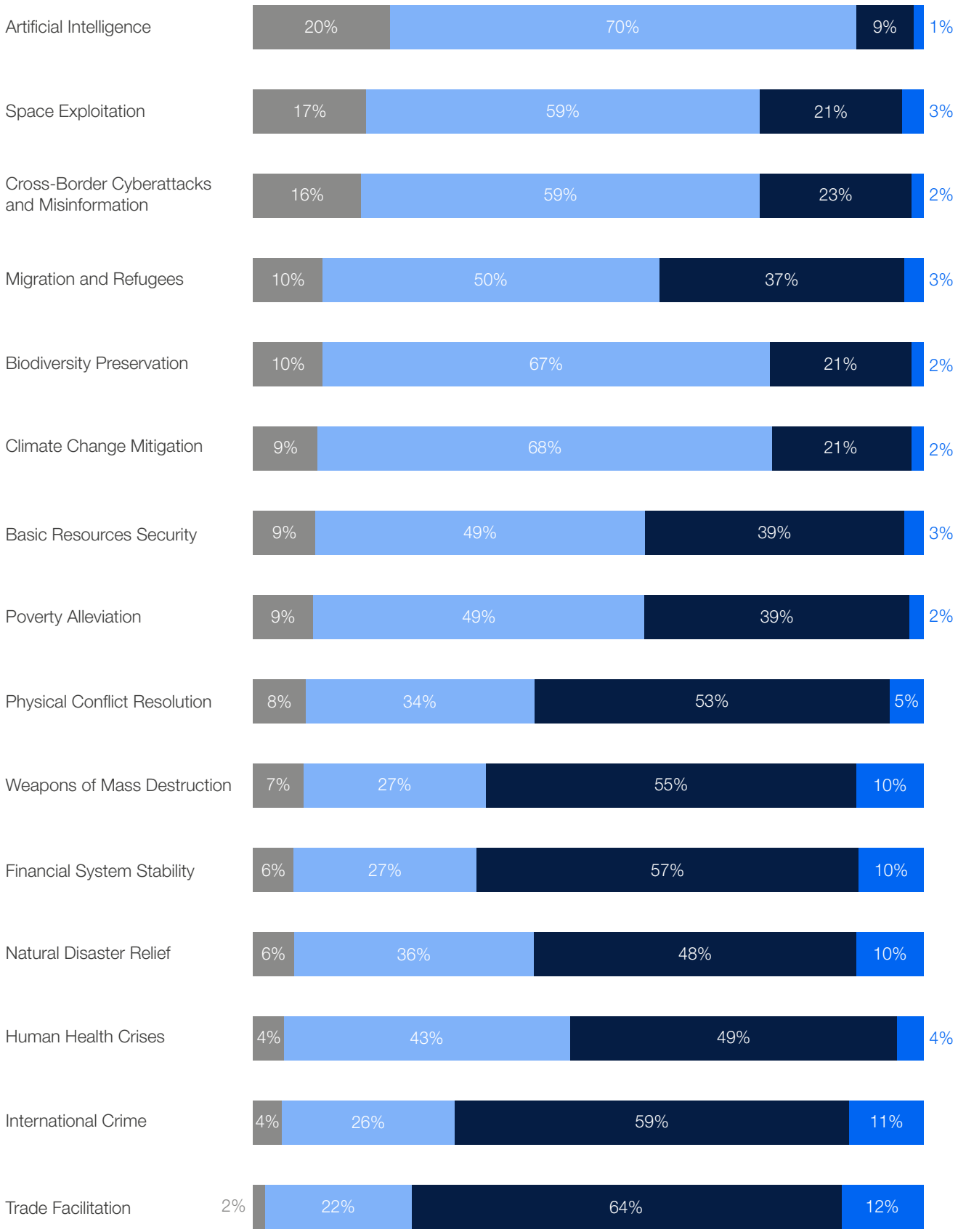


*Line thickness scaled according to tally of links (see Appendix C: Technical Notes).

FIGURE IV

International Risk Mitigation Efforts

Current state of international risk mitigation efforts in each area



Endnotes

1 WHO (World Health Organization). "WHO Coronavirus (COVID-19) Dashboard – 'persons fully vaccinated'". https://covid19.who.int/, accessed 3 January 2022.

2 Kemp, S. 2021. "Digital 2021 April Global Statshot Report". Datareportal. 26 April 2021. https://datareportal.com/reports/digital-2021-april-global-statshot

3 UNESCO (United Nations Educational, Scientific and Cultural Organization). 2021. "UNESCO warns 117 million students around the world are still out of school" Press Release. UNESCO. 16 September 2021. https://en.unesco.org/news/unesco-warns-117-million-students-around-world-are-still-out-school

4 Sedik, T. S. and Xu, R. 2020. "A Vicious Cycle: How Pandemics Lead to Economic Despair and Social Unrest". IMF Working Papers. IMF. 16 October 2020. https://www.imf.org/en/Publications/WP/Issues/2020/10/16/A-Vicious-Cycle-How-Pandemics-Lead-to-Economic-Despair-and-Social-Unrest-49806

5 WHO. "WHO Coronavirus (COVID-19) Dashboard – 'confirmed cases' and 'deaths'". https://covid19.who.int/, accessed 3 January 2022.

6 WHO. 2021. "New policy brief calls on decision-makers to support patients as 1 in 10 report symptoms of "long COVID"". Policy Brief. WHO. 25 February 2021. https://www.euro.who.int/en/health-topics/health-emergencies/coronavirus-covid-19/news/news/2021/2/new-policy-brief-calls-on-decision-makers-to-support-patients-as-1-in-10-report-symptoms-of-long-covid

7 Our World in Data. "Coronavirus (COVID-19) Vaccinations – 'By country'". https://ourworldindata.org/covid-vaccinations?country=OWID_WRL, accessed 3 January 2022.

8 Bloomberg. "More Than 8.23 Billion Shots Given: Covid-19 Tracker". https://www.bloomberg.com/graphics/covid-vaccine-tracker-global-distribution/, accessed 3 January 2022.

9 WHO. "WHO Coronavirus (COVID-19) Dashboard – 'confirmed cases'". https://covid19.who.int/, accessed 3 January 2022.

10 COVID-19 Mental Disorders Collaborators. 2021. "Global prevalence and burden of depressive and anxiety disorders in 204 countries and territories in 2020 due to the COVID-19 pandemic". The Lancet. Volume 398, Issue 10312. 6 November 2021. https://www.thelancet.com/journals/lancet/article/PIIS0140-6736(21)02143-7/fulltext#%20

11 WHO. 2021. "Noncommunicable diseases". Factsheet. WHO. 13 April 2021. https://www.who.int/news-room/fact-sheets/detail/noncommunicable-diseases

12 Knight, G.M., Glover, R.E., McQuaid, C.F., Olaru, I.D., Gallandat, K., Leclerc, Q.J., Fuller, N.M., Willcocks, S.J., Hasan, R,, van Kleef, E. and Chandler, C.I.R, 2021. "Antimicrobial resistance and COVID-19: Intersections and implications". Epidemiology and Global Health. eLife. 16 February 2021. https://elifesciences.org/articles/64139

13 IMF (International Monetary Fund). 2021. World Economic Outlook, October 2021: Recovery During a Pandemic Health Concerns, Supply Disruptions, and Price Pressures. October 2021. https://www.imf.org/en/Publications/WEO/Issues/2021/10/12/world-economic-outlook-october-2021

14 Ibid.

15 MarketWatch. "Bloomberg Commodity Index – YTD". https://www.marketwatch.com/investing/index/bcom?countrycode=xx, accessed 3 January 2022.

16 Cohen, A. 2021. "China's Energy Crisis Deepens with Potentially Fatal Consequences". Forbes. 19 October 2021. https://www.forbes.com/sites/arielcohen/2021/10/19/chinas-energy-crisis-deepens-with-potentially-fatal-consequences/?sh=4af8e5531163; Erlanger, S., Reed, S. and Troianovski, A. 2021. "As Europe faces a cold winter, Putin seizes on the leverage from Russia's gas output". New York Times. 7 October 2021. https://www.nytimes.com/2021/10/07/world/europe/putin-russia-natural-gas-europe.html;

17 World Economic Forum. 2021. "Chief Economists Outlook". WEF. November 2021. https://www3.weforum.org/docs/WEF_Chief_Economists_Outlook_November_2021.pdf

18 Kose, M. A., Ohnsorge, F. and Sugawara, N. 2021. "Navigating the debt legacy of the pandemic." Future Development. The Brookings Institution. 20 October 2021. https://www.brookings.edu/blog/future-development/2021/10/20/navigating-the-debt-legacy-of-the-pandemic/

19 Galouchko, K. 2021. "Fund managers sour on global growth expectations, BofA says". Bloomberg. 19 October 2021. https://www.bloomberg.com/news/articles/2021-10-19/bofa-survey-shows-fund-managers-slashing-bonds-to-a-record-low

20 MarketWatch. "U.S. Dollar Index (DXY) – YTD". https://www.marketwatch.com/investing/index/dxy, accessed 3 January 2022.

21 IMF. 2021. Op. cit.

22 International Labour Organization. 2021. "World Employment and Social Outlook. Trends 2021." ILO Flagship Report. ILO. 2021. https://www.ilo.org/wcmsp5/groups/public/---dgreports/---dcomm/---publ/documents/publication/wcms_795453.pdf

23 Deaton, A. 2021. "COVID-19 and Global Income Inequality". LSE Public Policy Review. London School of Economics Press. 3 May 2021. https://ppr.lse.ac.uk/articles/10.31389/lseppr.26/

24 Mahler, D. G., Lakner, C. and Yonzan, N. 2021. "Is COVID-19 increasing global inequality?". World Bank Blogs. World Bank. 7 October 2021. https://blogs.worldbank.org/opendata/covid-19-increasing-global-inequality#_ftnref1

25 Dooley, M. and Kharas, 2021. H. "Long-run impacts of COVID-19 on extreme poverty". Future Development. The Brookings Institution. 2 June 2021. https://www.brookings.edu/blog/future-development/2021/06/02/long-run-impacts-of-covid-19-on-extreme-poverty/

26 Institute of Politics and Public Service. McCourt School of Public Policy. 2021. "New Poll: Voter Frustration Fuels Sharp Drop in Approval for Biden and both Parties in Congress". Press Releases and Announcements. Georgetown University. 28 October 2021. https://politics.georgetown.edu/2021/10/28/new-poll-voter-frustration-fuels-sharp-drop-in-approval-for-biden-and-both-parties-in-congress/

27 Krastev, I. and Leonard, M. 2021. "Europe's Invisible Divides: How Covid-19 is Polarising European Politics". Policy Brief. European Council on Foreign Relations. September 2021. https://ecfr.eu/wp-content/uploads/Europes-invisible-divides-How-covid-19-is-polarising-European-politics.pdf

28 Reality Check Team. 2021. "Foreign aid: Who will be hit by the UK government cuts?". BBC News. 8 November 2021. https://www.bbc.com/news/57362816

29 Cordesman, A. H. and Hwang, G. 2021. "Updated Report: Chinese Strategy and Military Forces in 2021". Report. Center for Strategic and International Studies. 3 August 2021. https://www.csis.org/analysis/updated-report-chinese-strategy-and-military-forces-2021

30 IMF. Op. cit.

31 Bridge Consulting (Beijing) Co., Ltd. "China COVID-19 Vaccine Tracker". https://bridgebeijing.com/our-publications/our-publications-1/china-covid-19-vaccines-tracker/, accessed 7 December 2021.

32 World Bank. 2021. "International Debt Statistics 2022". Report. World Bank. 11 October 2021. https://www.worldbank.org/en/news/press-release/2021/10/11/low-income-country-debt-rises-to-record-860-billion-in-2020

33 Denyer, S. 2020. "Japan helps 87 companies to break from China after pandemic exposed overreliance". The Washington Post. 21 July 2020. https://www.washingtonpost.com/world/asia_pacific/japan-helps-87-companies-to-exit-china-after-pandemic-exposed-overreliance/2020/07/21/4889abd2-cb2f-11ea-99b0-8426e26d203b_story.html; Sikarwar, D.2021. "India set to erect a Great Wall against Chinese companies". The Economic Times. 19 June 2021. https://economictimes.indiatimes.com/news/economy/policy/india-set-to-erect-a-great-wall-against-chinese-companies/articleshow/76455684.cms?from=mdr

34 Climate Action Tracker. 2021. "Glasgow's 2030 credibility gap: net zero's lip service to climate action". The Climate Action Tracker. 11 November 2021. https://climateactiontracker.org/publications/glasgows-2030-credibility-gap-net-zeros-lip-service-to-climate-action/

35 Irfan, U. 2021. "What the world did and didn't accomplish at COP26". Vox. 13 November 2021. https://www.vox.com/22777957/cop26-un-climate-change-conference-glasgow-goals-paris

36 Hodgson, C., Hook, L. and Pickard, J. 2021. "India and China weaken pledge to phase out coal as COP26 ends". Financial Times. 13 November 2021. https://www.ft.com/content/471c7db9-925f-479e-ad57-09162310a21a

37 UN Climate Change Conference UK 2021. 2021. "Glasgow Leaders' Declaration on Forests and Land Use". UNFCCC. 2 November 2021. https://ukcop26.org/glasgow-leaders-declaration-on-forests-and-land-use/

38 Boadle, A. and Spring, J. 2021. "Brazil's Amazon deforestation surges to 15-year high, undercutting government pledge". Reuters. 19 November 2021. https://www.reuters.com/world/americas/brazil-deforestation-data-shows-22-annual-jump-clearing-amazon-2021-11-18/

39 Mountford, H., Waskow, D., Gonzalez, L., Gajjar, C., Cogswell, N., Holt, M., Fransen, T., Bergen, M. and Gerholdt, R. 2021. "COP26: Key outcomes from the UN Climate Talks in Glasgow". Reuters. 17 November 2021. https://www.wri.org/insights/cop26-key-outcomes-un-climate-talks-glasgow; Sengupta, S. 2021. "Calls for climate reparations reach boiling point in Glasgow talks". New York Times. 11 November 2021. https://www.nytimes.com/2021/11/11/climate/climate-glasgow-cop26-loss-damage.html

40 World Economic Forum, in partnership with Marsh & McLennan Companies, SK Group and Zurich Insurance Group. 2021. The Global Risks Report 2020. Insight Report. Chapter 2 Error 404: Barriers to Digital Inclusivity. Geneva: World Economic Forum. January 2021. https://www.weforum.org/reports/the-global-risks-report-2021

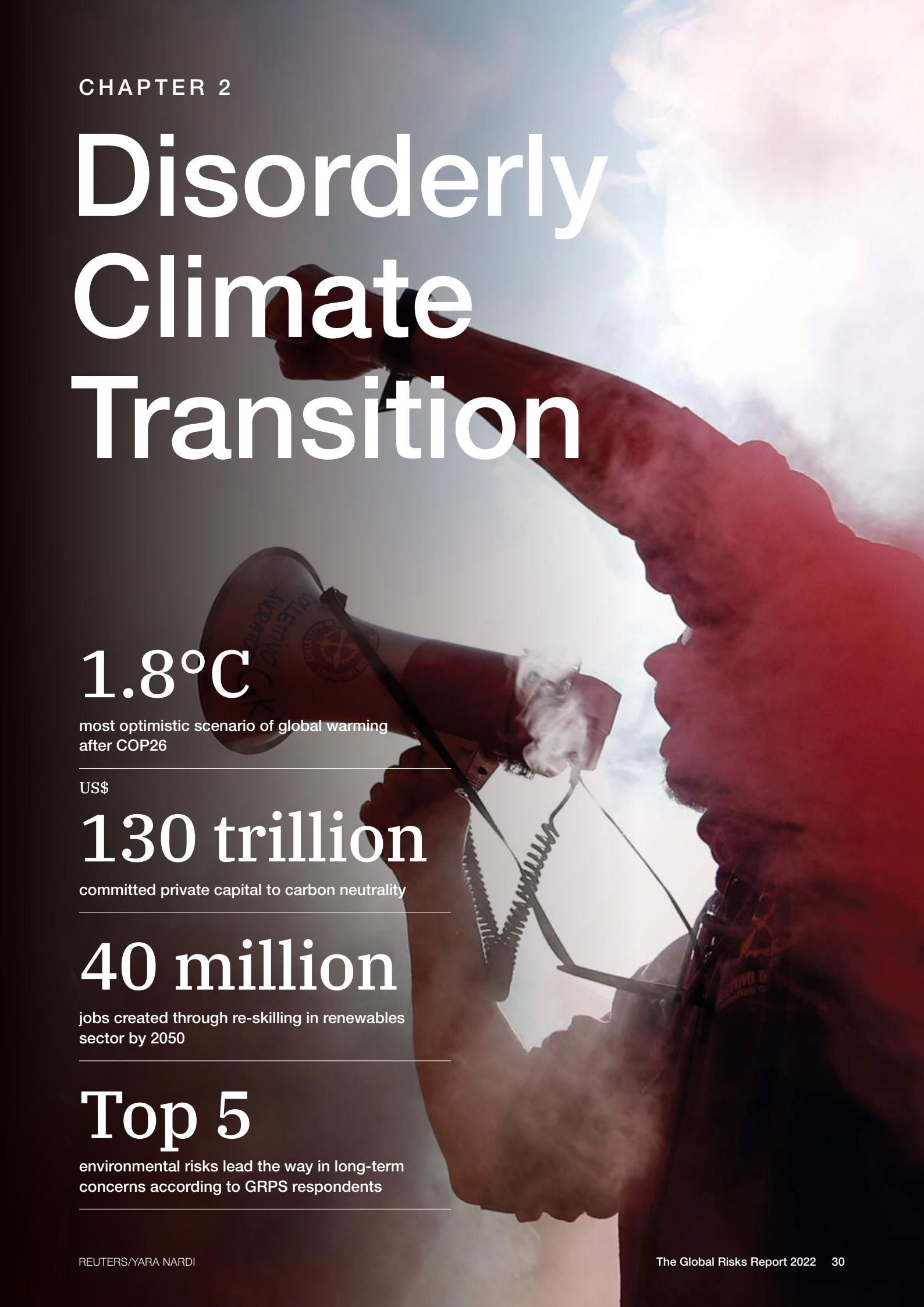
41 Balmforth, Tom. 2021. "'Razor-sharp precision': Russia hails anti-satellite weapons test". Reuters. 17 November 2021. https://www.reuters.com/business/aerospace-defense/russia-dismisses-us-criticism-anti-satellite-weapons-test-2021-11-16/; Stewart, P. 2021. "Top U.S. general confirms 'very concerning' Chinese hypersonic weapons test". 28 October 2021. https://www.reuters.com/business/aerospace-defense/top-us-general-confirms-very-concerning-chinese-hypersonic-weapons-test-2021-10-27/

42 UN DESA (United Nations, Department of Economic and Social Affairs). 2014. Global Governance and Global Rules for Development in the Post-2015 Era. Committee for Development Policy Policy Note. 16 June 2014. https://www.un.org/development/desa/dpad/publication/cdp-policy-note-2014/

43 Schwab, K. and Malleret, T, 2020, "COVID-19: The Great Reset", World Economic Forum. https://www.weforum.org/agenda/2020/07/covid-19-the-great-reset/

CHAPTER 2

Disorderly Climate Transition



1.8°C

most optimistic scenario of global warming after COP26

US$

130 trillion

committed private capital to carbon neutrality

40 million

jobs created through re-skilling in renewables sector by 2050

Top 5

environmental risks lead the way in long-term concerns according to GRPS respondents

REUTERS/YARA NARDI

Climate (in-)action

Accelerating and widespread climate change manifests itself in irreversible consequences.[1] The overwhelming weight of scientific analysis points to environmental adjustments and cataclysmic feedback loops that will push ecosystems beyond tipping points.[2] At that moment, decarbonization efforts would be rendered mute.

The latest nationally determined contributions (NDCs) to decarbonization made at the 2021 United Nations Climate Change Conference of the Parties (COP26) still fall short of the 1.5°C goal set out in the Paris Climate Agreement (for an extensive summary of COP26 outcomes, see Chapter 1, Box 1.1).[3] The current trajectory is expected to steer the world towards a 2.4°C warming,[4] with only the most optimistic of scenarios holding it to 1.8°C (see Figure 2.1).

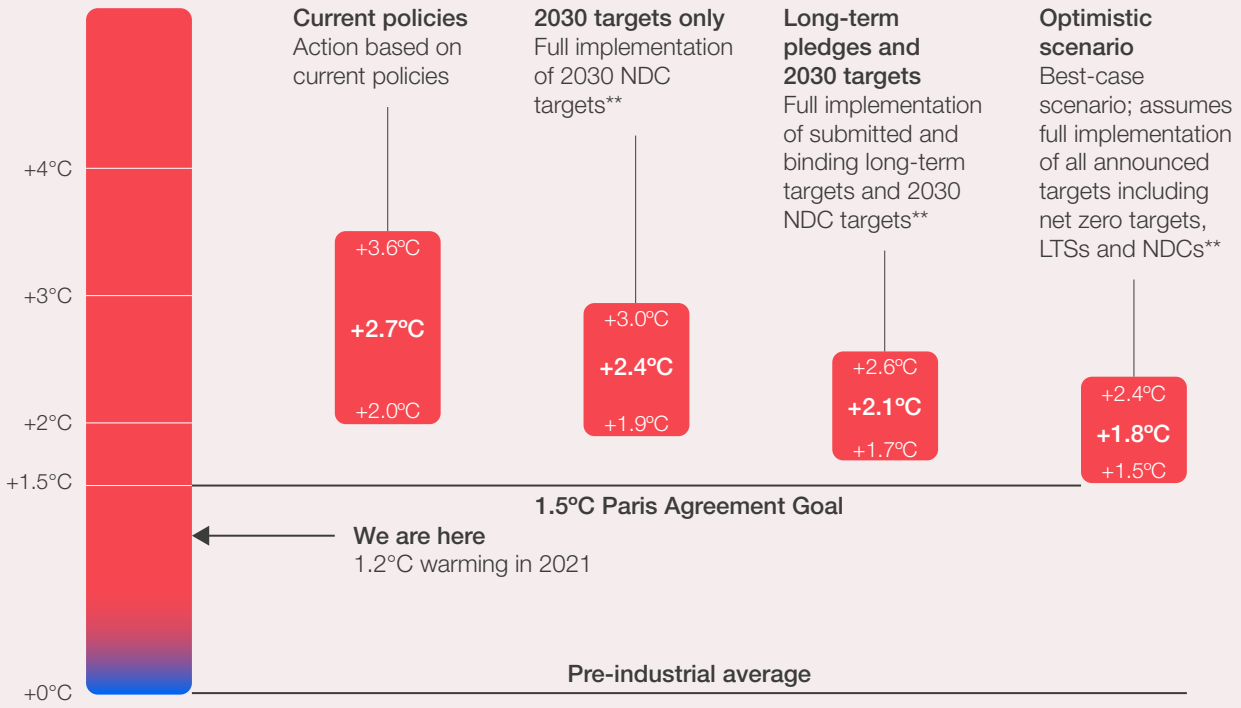
Without stronger action, global capacity to mitigate and adapt will be diminished, eventually leading to a "too little, too late" situation and ultimately a "hot house world scenario" with runaway climate change that makes the world all but uninhabitable.[5] The world will face high costs if we collectively fail to achieve the net zero goal by 2050.[6] Complete climate inaction will lead to losses projected to be between 4% and 18% of global GDP[7] with different impacts across regions.[8]

The transition to net zero—the state in which greenhouse gases (GHG) emitted into the atmosphere are balanced by their removal from the atmosphere*—could be as transformative for economies and societies as past industrial revolutions. However, the complexities of the technological, economic and societal

* Net zero carbon dioxide (CO_2) emissions are achieved when anthropogenic CO_2 emissions are balanced globally by anthropogenic CO_2 removals over a specified period. Net zero CO_2 emissions are also referred to as "carbon neutrality." This definition of "net zero" is from the IPCC (Intergovernmental Panel on Climate Change). 2018: Annex I Glossary. https://www.ipcc.ch/sr15/chapter/glossary/

FIGURE 2.1

Global Temperature Scenarios by 2100



** Nationally determined contributions (NDCs) are non-binding national plans for climate action, including targets for GHG emissions reductions. Long-term strategies (LTSs) are national mid-century development plans for confronting climate change. If 2030 NDC targets are weaker than projected emissions levels under current policies, then current policies are used here.

Source: Based on the Climate Action Tracker. https://climateactiontracker.org/

changes needed for decarbonization, coupled with the slow and insufficient nature of current commitments, will inevitably lead to varying degrees of disorderliness.

As climate change intensifies and some economies recover more quickly than others from COVID-19, a disorderly transition could bifurcate societies and drive countries further apart, and a too-slow transition will only beget damage and disruption across multiple dimensions over the longer term (see Box 2.1). Within countries, the disruptive potential of the transition could be amplified by disconnects between governments, businesses and households with respect to policy commitments, financial incentives, regulations and immediate needs. A sustained lack of coordination between countries would likely have profound geopolitical implications, with rising friction between strong decarbonization advocates and those who oppose quick strong action by using tactics such as stalling climate action or greenwashing— the practice of making people believe that a company or authority is more environmentally friendly than it actually is.

Tailwinds for a fast, but disorderly, transition

Clear evidence of rising physical risks, such as melting land ice, rising sea levels and prolonged periods of extreme heat and cold,[9] as well as their associated consequences for human and economic systems,[10] are intensifying momentum for the transition. And while COVID-19 lockdowns saw a global dip in GHG emissions, upward trajectories soon resumed:[11] GHG emissions rates rose faster in 2020 than their average over the last decade,[12] illustrating how the global economy is still heavily dependent on fossil fuels.

COVID-19 lockdowns saw a global dip in GHG emissions. However, upward trajectories soon resumed

Governments, businesses, investors and communities are increasingly converging on the need for a quicker transition—each group setting higher expectations of the other. Green parties and green policies—such as a carbon border adjustment tax[13]—have gained traction in many countries, regions and industries, as have multilateral ideas like climate clubs.[14] A plethora of climate risk disclosure frameworks and measurement standards are now being combined within a new International Sustainability Standards Board (ISSB) by the International Financial Reporting Standards (IFRS). This will help clarify what needs to be done, and by whom, to highlight and prevent greenwashing and stalling on climate action.

The rise of stakeholder capitalism, shareholder activism and increased appetite from companies to use environmental,

BOX 2.1

Global Risks Perception Survey Ranks "Climate Action Failure" as Top Risk

Respondents to the Global Risks Perception Survey (GRPS) 2021–2022 rank "climate action failure" as the most critical threat to the world in both the medium term (2–5 years) and long term (5–10 years), with the highest potential to severely damage societies, economies and the planet. Most also believe too little is being done: 77% said international efforts to mitigate climate change have "not started" or are in "early development". (The survey was conducted before COP26. See Appendix C, Technical Notes).

REUTERS/PRAPAN CHANKAEW

social and governance (ESG) targets and metrics,[15] coupled with ESG-based investments, is re-shaping the financial and economic landscape,[16] and an increasing number of organizations are committing to decarbonize their operations. As banks, insurers and institutional investors are steering capital towards net zero, financial systems are rapidly emerging as critical enablers of the transition. A growing share of the US$100 trillion bond market is mobilized for climate change solutions, and it is expected to reach the milestone of US$1 trillion in annual issuances by 2022.[17] Moreover, during COP26, the Glasgow Financial Alliance for Net Zero (GFANZ) announced that over US$130 trillion in private capital has been committed to carbon neutrality—enough to achieve net zero by 2050.[18] Similarly, parties at COP26 agreed on the framework for Article 6 of the Paris Agreement, enabling the immediate operationalizing of global carbon markets, ending uncertainty about the Clean Development Mechanism (CDM) and further establishing a new central UN supervisory body to trade carbon credits on specific projects.

These commitments by both businesses and governments are being closely monitored by civil society organizations and investors,[19] which fear untenable populist promises are being made for short-term political or financial gain.[20]

Headwinds slowing the transition

The risk of a disorderly transition is aggravated by the interdependencies and distributed nature of economic and financial systems, the historic shielding of climate change externalities from citizens and businesses, decarbonization costs, and the many divergent interests at play that will complicate the transition. In the short term, these complexities are likely to prompt many actors to avoid or defer action.

Some national and business actors are still deliberately manoeuvring to stall or scale back the green transition. Governments need to balance the needs of populations dependent on carbon-intensive industries with international commitments. Yet some

of these commitments are lofty and lacking scientific credibility,[21] legislatures are pre-emptively blocking new climate laws,[22] and regulations are being contested in courts by both proponents who push for more climate action and those who advocate for less.[23] Geopolitical tensions and rising competition over climate-friendly raw materials also further threaten to undermine international cooperation on green transition progress.[24] Some actors show little interest in the multilateral platforms on which climate action is taking place;[25] others continue to prioritize nationally important industries and could, in the wake of increased global tensions, shift to national security concerns over action on the transitions.

With government finances under pressure, regulatory obligations are not going far or fast enough, and there is an assumption that market forces will come to the rescue. In many countries there are insufficient incentives for households and businesses to invest in net zero technologies and few penalties for failing to do so. Slow uptake of new technologies such as low-carbon energy generation and carbon capture and storage, continued household overconsumption of carbon-intensive products and services,[26] and a failure to grasp the seriousness of climate threats all point to a slower transition that preserves "order" in the near term.[27] New innovations that require high amounts of energy during production and use, such as crypto-mining or crypto-trading,[28] often coming from fossil fuel energy sources, can also offset efforts to reduce ecological footprints.

Post-COVID-19 recovery measures mostly neglect the green transition in favour of short-term stability

Post-COVID-19 recovery measures mostly neglect the green transition in favour of short-term stability,[29] while loose monetary policies further distort green, market-based solutions or investments;[30] they also exacerbate the problem of zombie companies.[31] Carbon-intensive technologies continue to receive public subsidies,[32] with over 50 developed and emerging economies committing US$345 billion to fossil fuels in 2020—a figure lower than in previous years largely because of depressed consumption and prices during the pandemic.[33] At the time of writing, the economic rebound following the impact of COVID-19 has seen (fossil) energy demand outstrip supply,[34] resulting in sharply increased energy prices, even as the world turns against fossil fuels.[35] Moreover, some business actors continue their efforts to slow the transition. Climate-sceptic lobbying,[36] greenwashing and sowing misinformation and distrust about climate science remain pervasive in many countries.[37]

GETTY/SCHROPTSCHOP

Some economic incentives also complicate attempts to coordinate measures that could internalize costs in high-emission industries and countries, minimize market disruptions and more fairly redistribute burdens and rewards. Instead of fostering decarbonization, the lack of global emission prices and reporting requirements continues to shield consumers and producers from the cost of inaction.[38] This incentivizes countries and businesses not to curb emissions, but instead to game the system and avoid liability by offshoring carbon-intense activities or trading their emissions to countries with less stringent regulations.[39] Developing countries attracted to emissions in-shoring schemes by short-term financial gain squander the opportunity to use carbon allowances for their own development and risk undermining their future access to trade flows and the finance needed for mitigation and adaptation.[40]

Businesses may be unprepared for transition risks such as rapid shifts in policies and regulations, the need to develop low-carbon technologies and changes in consumer behaviour and investor preferences.[41] These risks have the potential to destabilize the financial system,[42] as in aggregate they can increase default rates and asset volatility. They are further amplified in economies with low investment capability, high reliance on fossil fuels and less-inclusive political systems.[43]

Consequences

The consequences and repercussions of the transition will necessarily reflect the speed at which it takes place; the efforts that go into it; and whether it is slow or aggressive, concerted or entrenched, and focused more on mitigation or adaptation. The goal of 1.5°C is so fundamental that societies need to be prepared to assume negative consequences of policies taken by governments today to avoid the worst consequences tomorrow. This includes job losses, increased costs and geopolitical insecurity associated with a disorderly transition. Only a socially just transition will make the consequences bearable for large parts of societies with governments needing to create policies and social-protection systems that help reduce the impacts for those affected. A rapid decarbonization would increase economic and societal disruption in the short term, while a slower pace with fewer short-term impacts would entail much larger costs and greater disorderliness in the long-term.

GRPS respondents drew attention to the societal consequences of environmental degradation at a global scale. They identify "climate action failure" and "extreme weather" as strong aggravators of "involuntary migration", "livelihood crises" and "social cohesion erosion". In contrast, respondents to the Executive Opinion Survey (EOS) see the impacts from "climate action failure" as top risks in the short-term at a country level: "human environmental damage" and "extreme weather" are considered top-10 risks in 90 economies and 60 countries, respectively. All countries ranking these risks highly are particularly prone to wildfires, droughts, floods, deforestation and pollution.

Varying speeds

A hasty pace

Concerted, aggressive action now will, because of the scale of the endeavour, bring discontinuities and thus disruptions, as efforts within and between industries, businesses and governments fail to align. It would alleviate long-term environmental consequences but could have severe short-term economic and societal impacts. Missteps will likely threaten national energy security, for example, and result in volatile energy prices. Over the longer term, countries will face questions regarding the viability of vehicle fuel and gas supply arrangements when much of the population has shifted away from combustion engines, gas boilers and heating.

GETTY/AERIAL PERSPECTIVE WORKS

As carbon-intense industries employ millions of workers, their rapid termination could trigger economic volatility and increase societal and geopolitical tensions. Up to 8.5 million jobs in the energy sector (almost 30%) could be lost in fossil fuels and nuclear energy by 2050, although with re-skilling up to 40 million new jobs could be created, mostly in renewables.[44] Earlier or current investments in carbon-intensive technologies could result in stranded assets. These—even if they are the result of wilfully made investments in carbon-intensive technologies for short-term gain instead of long-term investments in clean technologies[45]—could impact the financial sector,[46] as well as the transition, when they are trapped in industries such as those that extract resources required for low-carbon technologies.[47] Despite these short-term disruptions, the social and economic consequences of unmitigated global warming and entire nations being flooded or disappearing would be even more cataclysmic: countries' complete economies and assets would be left stranded.

Non-holistic government approaches also pose risks. Adopting low-carbon and more sustainable technologies too hastily, in a way that neglects systemic interdependencies—such as transitioning one system before another linked or dependent one is ready—could lead to production shortages and disrupt secondary economic cycles if redundant systems are not in place to prevent energy supplies from collapsing. Poor regulation of new green markets could create unwanted monopolies in geopolitically contested industries such as rare earth elements extraction.

Some approaches to the green transition reflect blind spots that risk damaging outcomes for workers and the environment.[48] These include focusing solely on carbon dioxide (CO_2) emissions and ignoring methane,[49] or the increased use of resources for low-carbon technologies. They also risk setting regulatory requirements to phase out technologies before substitutes exist or, in other words, a focus on supply constraint of fossil fuels rather than an equal emphasis on demand-destruction in the most carbon-intensive industries.

Slow transition

In contrast, a slower but more orderly transition might be more manageable in the short term but would result in the need for deeper and faster changes by 2050. This would lead to more pronounced long-term disorder, amplified at the same time by more damaging economic activity such as the closing off of opportunities, damaging impacts through environmental degradation impacting societal well-being and infrastructural fragilities.

The long-term financial impacts would disproportionately affect large and/or developing countries.[50] Some of these countries face political and financial barriers to swiftly reducing their reliance on fossil fuel energy production such as cutting coal use;[51] others rely on natural gas to

reach a higher level of industrialization before decarbonizing,[52] even though these policies further aggravate the destruction of ecosystems. Consequently, the loss of (arable) land would increase migration pressure and the number of climate refugees (see Chapter 4). This slow pathway may lead countries to prioritize adaptation over mitigation efforts. Yet, once carbon prices increase and demand destruction ends up making fossil energy investment a losing bet, leapfrogging to renewables sooner than later could prove to be a more effective long-term investment for such developing countries.

Divergent paces

It is most likely that national transition programmes will move at different paces as a result of differences in political will (decarbonization ambitions and political interest), economic structure (service versus manufacturing) and capabilities (technological know-how and financial wherewithal). Countries that move faster will be able to consolidate their own national capabilities and clean tech industries; those that move more slowly will lack competitiveness in this area but be able to leverage the best that has been developed elsewhere. Initiatives that pay closer attention to scope 3* emissions will shine a spotlight on global value chains and will increasingly disadvantage exports from laggard countries. Furthermore, the heterogeneity of climate action worldwide will be a risk for trade flows in the future, especially for the less-developed economies. By facing narrower access to trade finance, they risk exclusion from the opportunities for orderly climate mitigation and adaption.[53]

Reputational damage and liability issues for governments and businesses seen as complicit in, if not responsible for, climate change could lead to breakdowns in trust between nations, higher global tensions and the possibility of sanctions being introduced against laggard nations, or fines/trade tariffs against relapsing businesses.

Transition policies risk losing public support if they neglect the impacts—on land use, resources, nature—of large-scale water and wind energy installations,[54] or emanate from failure to create just pricing schemes for communities willing to invest in green energy, such as a shift of fossil fuel to renewable energy subsidies or equal feed-in tariffs for individuals and large-scale providers.[55] Poor grid stability through the intermittency of renewable energy sources, shortages in storage capacity and the phasing out of existing baseload energy technologies that have a low carbon intensity yet are politically highly controversial, such as nuclear energy,[56] could also dwindle public support for cleaner energy sources.

Especially at risk are unskilled workers unable to transition their skill sets

Biotechnical and geoengineering solutions

While negative emission technologies are an essential component of all IPCC 1.5°C scenarios, geoengineering solutions could be silver-bullet solutions, but they may not adequately explore systemic interdependencies and implications.[57] Moreover, the deployment of such untested technologies carries unknown risks. Some geoengineering approaches—such as weather modification or solar radiation management (SRM)—could spiral out of control or create friction if they are used for geopolitical advantage in the absence of any governance framework,[58] as the effectiveness could vary regionally.[59] They could exacerbate geopolitical tensions between countries where the local climate is improving and those that are suffering from the unintended consequences.[60]

On the other side, biotechnical solutions such as carbon dioxide removal (CDR)

* Scope 1 emissions are direct emissions from owned or controlled sources. Scope 2 emissions are indirect emissions from the generation of purchased energy. Scope 3 emissions are all indirect emissions (not included in scope 2) that occur in the value chain of the reporting company, including both upstream and downstream emissions. This definition of "Scope 3 emissions" is from the Greenhouse Gas Protocol. 2021. https://ghgprotocol.org/sites/default/files/standards_supporting/FAQ.pdf

from the atmosphere need to be scaled up to come close to keeping the 1.5°C scenario within reach under all IPCC scenarios.[61] The robustness of any net zero strategy that relies on CDR depends both on the effectiveness of the underlying projects that drive the CO_2 removal and, especially, on the permanence of the stored carbon.[62] Other solutions, such as carbon capture, utilization and storage (CCUS), are already heavily subsidized,[63] but they risk being used for greenwashing as carbon-heavy industries eventually fail to structural change their value chains to reduce their emissions.[64] Similarly, Bio-energy Carbon Capture and Storage (BECCS) solutions could create unintended geopolitical consequences or prove to be counterproductive. [65]

Stakeholder consequences

Loss of agency: Consequences for individuals

The type of transition will have far-reaching socio-economic implications for individuals. Where policies, incentives and innovations fail to stimulate effective market solutions, households will see increases in their cost of living due to rising decarbonization requirements for homes, rising fossil fuel prices and physical climate impacts, among other issues. They may also face increased service disruption from utilities where system dependencies and discontinuities have not been adequately anticipated by participants. Especially at risk are unskilled workers, those unable to transition their skill sets and those currently employed in carbon-intensive industries that undergo radical transformation.[66] Many of these workers are already facing challenges related to automation and the hyper-globalization of the pre-COVID-19 era, when key heavy industries such as coal and steel were offshored to emerging markets.[67] Middle-class households could also be left behind if aggressive transition measures impact their finances and their purchasing power diminishes substantially.

Loss of income would inhibit people's access to new technologies and upward mobility, entrenching inequalities for generations. Unequal transition speeds could widen inequalities between economies and create pressure on workers to migrate to countries where their skills are still in demand (see Chapter 4). Failed or slow climate action could worsen gender inequalities as, in many low-income economies, women are responsible for gathering and producing

GETTY/VISOOT UTHAIRAM

REUTERS/OCTAVIO JONES

food, securing water and collecting bioenergy sources such as firewood and crop waste. Together, these consequences could trigger disillusionment with climate action and lead to the radicalization of marginalized socio-economic groups across the political spectrum.

Loss of control: Consequences for governments

Governments will face backlash whether climate action is slow or aggressive. Steeper transition costs such as high and quick increase in the price of carbon and fossil fuels could weaken public support for fast action; conversely, slow action could trigger further radicalization from those who feel authorities at all levels do not act fast enough, with a potential increase in inter-generational friction and more fiscal drain due to increased recovery funding. Investing in a net zero economy could create unsustainable levels of debt for economies lacking the means of such large-scale investment, or the loss of rent/tax revenue for economies heavily dependent on carbon intensive resource production, which would cripple public finances already vulnerable from the economic impacts of COVID-19 fallouts (see Chapter 1). Especially at risk are more climate-vulnerable countries; such green investment could be seen as a diversion from pandemic-related recovery programmes and the enhancement of core public infrastructure and services. Unequal access to low- or zero-carbon innovations could undermine support for governments in some countries.[68]

A socially unjust transition would exacerbate geopolitical and economic friction and inequalities between countries and regions. Laggard economies—especially those reliant on carbon-intensive sectors and that fail to keep up with technological innovation—risk losing competitive advantage and leverage in trade agreements, civil unrest, regime change and massive economic and societal disruption. Unequal access to materials and funding to enable the transition could increase tensions, as could unintended consequences—such as the destruction of ecosystems in developing countries to extract resources for next-level electrification of mobility in developed economies.[69]

Failed or delayed financial promises by advanced economies—such as a decline in promised foreign direct investment (FDI),[70] or shortcomings to the globally agreed annual $100 billion for emerging and developing countries to finance their transition to lower emissions and adaption measures to the physical consequences of climate change[71]—could leave developing countries stranded with costly, aggressive transition plans, unable to provide for vulnerable populations.

A zero-sum political game, with a first-come, first-served mentality, compounded by a lack of solidarity and combined with the absence of clear climate governance or enforceable accountability measures would increase tensions between economies transitioning quickly and those preferring or needing a slower transition.

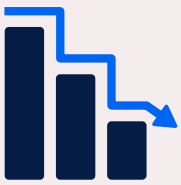
Loss of market share: Consequences for businesses
Policies triggering the premature termination of large-scale industries would disrupt markets, affect financing mechanisms and limit investment opportunities.[72]

Inconsistent policy signals, choices crippling competitiveness, and conflicting rhetoric, regulations and incentives would generate discontent among businesses. The transition could lead to stranded assets in carbon-intensive industries,[73] while devaluations could potentially affect the financial system,[74] leading to loss of liquidity and increasing liability, credit and market risks.[75] Businesses perceived as lagging, or as complicit in slowing down climate action,[76] could lose consumer and investor confidence and face additional state intervention and liability risk through judicial action.[77] Overall, businesses could also lose out on opportunities to invest in net zero technologies and the skilled professionals of the future,[78] impacting their long-term viability.

A disorderly transition could see more frequent and severe supply chain disruptions due to labour and product shortages, especially as sectors and companies switch operating models or simply go out of business. These disruptions present challenges to the resilience of business models across all industries.

Loss of nature
How the speed and degree of transition impacts natural ecosystems will, in turn, help or hinder its effectiveness. Some actions taken to mitigate climate change will incur costs for nature. In the rush to increase biomass use for BECCS, to use more agricultural land to create biofuels for industries such as aviation, and to extract minerals needed for the decarbonization of the world's economy,[79] additional negative impacts on ecosystems and indigenous societies in emerging economies are difficult to avoid. Solutions used for carbon offsetting, such as restoring or reforesting land—so-called offset forests—could be destroyed if that land is damaged by more severe weather such as wildfires or floods, eventually unleashing the stored carbon. Poorly sited windfarms or hydroelectric dams can affect ecosystems and wildlife at a large scale, and they also present societal risks (such as forced relocation of local residents) and political risks (such as by controlling downstream water-access to neighbouring countries). The continued degradation of nature will add to stress on local residents, public health, businesses and ultimately the stability of society, while regional population growth will further impact the use of land and resources such as water and food.

Shocks to Reflect Upon

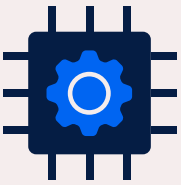


Green Market Crash

What if the boom in sustainable investments becomes a bubble, followed by a crash that cripples innovation and progress?

Fusion Power at Last

What if a new transformative technology emerges but cannot be mass-produced at low cost, disadvantaging developing economies and impacting climate action dynamics?



Collateral Geo-Damage

What if unilateral implementation of large-scale geoengineering solutions creates unexpected knock-on effects that developing economies are ill-equipped to handle?

Towards a more sequenced transition

Beyond the sheer scale, complexity and interdependency of the needed changes, the climate transition will be disorderly because decades of inaction and hesitant implementation of transition measures on local and global levels have steered the planet onto a path that will be difficult to change.

In a recovering yet diverging global economy, countries will need to transition at varying paces to prevent short-term disruptions from offsetting long-term gains, but the consequences of disparate transitions will be felt worldwide. The least disruptive climate transition measures will be those that holistically integrate the needs of individuals, societies, businesses and planet. Domestic and international collaboration should focus on educating the public about the value and need of climate action, including a change in consumer behaviour and demand-destruction for carbon intensive goods. Businesses of all sizes need to be incentivised to proactively factor in transition risks and move to circular economy models, while governments should be encouraged to take bold and immediate steps towards implementing robust legal frameworks that ensure a just transition.

Any transition of this scale will be disruptive. All stakeholders need to focus on actions that will drive an innovative, determined and inclusive transition in order to minimize the impacts of disorder, facilitate adaptation and maximize opportunities.

GETTY/BLOOMBERG

Endnotes

1 IPCC (Intergovernmental Panel on Climate Change). 2021. "Climate Change 2021: The Physical Science Basis". Contribution of Working Group I to the Sixth Assessment Report of the Intergovernmental Panel on Climate Change. Cambridge University Press. In Press. https://www.ipcc.ch/report/ar6/wg1/

2 Elwin, P. and Baldock, Ch. 2021. "No rain on the plain: Deforestation threatens Brazil's agricultural exports". Planet Tracker. Briefing Paper, September 2021. https://burness.com/assets/pdf_files/no-rain-on-the-plain.pdf; World Economic Forum, in partnership with Marsh & McLennan Companies and Zurich Insurance Group. 2020. The Global Risks Report 2020. Insight Report. Chapter 4 Save the Axolotl. Geneva: World Economic Forum. January 2020. https://www.weforum.org/reports/the-global-risks-report-2020

3 Climate Action Tracker. 2021. "Glasgow's 2030 credibility gap: net zero's lip service to climate action". The Climate Action Tracker. 11 November 2021. https://climateactiontracker.org/publications/glasgows-2030-credibility-gap-net-zeros-lip-service-to-climate-action/

4 Ibid.

5 NGFS (Network for Greening the Financial System). Climate Scenarios for Central Banks and Supervisors. June 2020. NGFS Publications. https://www.ngfs.net/en/ngfs-climate-scenarios-central-banks-and-supervisors

6 Ricke, K., Drouet, L., Caldeira, K. and Tavoni, M. 2018. "Country-level social cost of carbon." Nature Climate Change, 8, 895–900. https://www.nature.com/articles/s41558-018-0282-y

7 Swiss Re. 2021. "World economy set to lose up to 18% GDP from climate change if no action taken, reveals Swiss Re Institute's stress-test analysis". 22 April 2021. https://www.swissre.com/media/news-releases/nr-20210422-economics-of-climate-change-risks.html

8 Swiss Re. 2021. The Economics of Climate Change: No Action Not an Option. Swiss Re Institute. April 2021. https://www.swissre.com/dam/jcr:5d558fa2-9c15-419d-8dce-73c080fca3ba/SRI_%20Expertise_Publication_EN_LITE_The%20economics_of_climate_change.pdf

9 IPCC. 2021. Op. Cit.

10 Bevere, L. and Weigel, A. 2021. "Sigma 1/2021 - Natural catastrophes in 2020". Swiss Re Institute. 30 March 2021. https://www.swissre.com/institute/research/sigma-research/sigma-2021-01.html

11 Carbon Monitor. 2021. https://carbonmonitor.org/ accessed 10 December 2021.

12 WMO (World Meteorological Organization). 2021. Greenhouse Gas Bulletin: The State of Greenhouse Gases in the Atmosphere Based on Global Observation through 2020. No. 17, 25 October 2021. https://library.wmo.int/doc_num.php?explnum_id=10904

13 European Commission. 2021. "Carbon Border Adjustment Mechanism". European Commission, 14 July 2021. https://ec.europa.eu/taxation_customs/green-taxation-0/carbon-border-adjustment-mechanism_de

14 Nordhaus, W. 2015. "Climate Clubs: Overcoming Free-riding in International Climate Policy". American Economic Review, 2015, 105(4): 1339-1370. https://www.aeaweb.org/articles?id=10.1257/aer.15000001.

15 World Economic Forum. 2020. Measuring Stakeholder Capitalism: Towards Common Metrics and Consistent Reporting of Sustainable Value Creation. September 2020. https://www.weforum.org/reports/measuring-stakeholder-capitalism-towards-common-metrics-and-consistent-reporting-of-sustainable-value-creation

16 Bartalos, G. 2021. "Advisors are underestimating retail demand for ESG investments". RIA Intel. 12 April 2021. https://www.riaintel.com/article/b1rcsns61lvt8t/advisors-are-underestimating-retail-demand-for-esg-investments; CFA Institute. 2020. "Future of sustainability in investment management: From ideas to reality". CFA Institute, Future of Finance. https://www.cfainstitute.org/-/media/documents/survey/future-of-sustainability.ashx; Reid, J. and Birgden, H. 2021. "Investing in a net-zero emissions transition". Marsh McLennan. https://www.marshmclennan.com/insights/publications/2021/september/investing-in-a-net-zero-emissions-transition.html

17 Fatin, L. 2021. "$1Trillion annual green bond milestone tipped for end 2022 in latest survey: Sean Kidney calls for $5Trillion per year by 2025". Climate Bonds Initiative. 28 October 2021. https://www.climatebonds.net/2021/10/1trillion-annual-green-bond-milestone-tipped-end-2022-latest-survey-sean-kidney-calls

18 GFANZ (Glasgow Financial Alliance for Net Zero). 2021. "Amount of finance committed to achieving 1.5°C now at scale needed to deliver the transition". 3 November 2021. https://www.gfanzero.com/press/amount-of-finance-committed-to-achieving-1-5c-now-at-scale-needed-to-deliver-the-transition/

19 Climate Action 100+. 2021. Net-Zero Company Benchmark. https://www.climateaction100.org/progress/net-zero-company-benchmark/; UN. 2021. "Nationally determined contributions under the Paris Agreement". UN Framework Convention on Climate Change, Synthesis report by the secretariat. 17 September 2021. https://unfccc.int/sites/default/files/resource/cma2021_08_adv_1.pdf

20 Bündnis90/Die Grünen. 2021. Deutschland – Alles ist drin: Bundestagswahlprogramm 2021. https://cms.gruene.de/uploads/documents/Wahlprogramm-DIE-GRUENEN-Bundestagswahl-2021_barrierefrei.pdf; Edgecliffe-Johnson, A., and Mundy, S. 2021. "Big business and COP26: Are the 'net zero' pans credible?". Financial Times. 21 November 2021. https://www.ft.com/content/d91b5934-de9e-4eef-a008-697bce53263f

21 Angelo, M. 2020. "Brazil's updated climate plan seen lacking credibility as forests shrink". Reuters. 10 December 2020. https://www.reuters.com/article/brazil-climate-change-idUSKBN28K1W6; Harvey, F., Watts, J. and Ni, V. 2011. "China's new climate plan falls short of Cop26 global heating goal, experts say". The Guardian. 28 October 2021. https://www.theguardian.com/environment/2021/oct/28/disappointing-but-not-unexpected-china-climate-goal-leaves-experts-unsatisfied

22 Leber, R. 2021. "An 'attack on American cities' is freezing climate action in its tracks". Vox. 29 September 2021. https://www.vox.com/22691755/gas-utilities-fight-electrification-preemption

23 Court of The Hague. 2021. C/09/571932 / HA ZA 19-379. C/09/Shell. https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBDHA:2021:5339; Taft, M. 2021. "The Supreme Court may fuck over the climate, too". Gizmodo. 29 October 2021. https://gizmodo.com/the-supreme-court-may-fuck-over-the-climate-too-1847966561

24 Megerian, C., and Su, A. 2021. "What U.S.-China tension means for fighting climate change". Los Angeles Times. 27 October 2021. https://www.latimes.com/politics/story/2021-10-27/china-united-states-climate-cooperation; White, E. 2021. "China says US tensions threaten fight against climate change". Financial Times. 2 September 2021. https://www.ft.com/content/5e830153-1e1a-4dfb-b40a-8469384ab6d0;

25 Colson, T. 2021. "Xi and Putin are snubbing the COP26 climate summit, even though China and Russia produce some 32% of global CO2 emissions". Business Insider. 25 October 2021. https://www.businessinsider.com/china-xi-and-russia-putin-snubbing-cop26-2021-10?r=US&IR=T

26 Deloitte. 2021. "How COVID-19 changes consumer behavior long-term". Monitor Deloitte. https://www.deloitte-mail.de/custloads/141631293/md_1804032.pdf

27 World Economic Forum, in Partnership with SAP and Qualtrics. 2021. The Climate Progress Survey: Business and Consumer Worries and Hopes. November 2021. https://www3.weforum.org/docs/SAP_WEF_Sustainability_Report.pdf

28 Bogna, J. 2022. "What is the environmental impact of cryptocurrency?" PCmag. 8 January 2022. https://uk.pcmag.com/old-cryptocurrency/138047/what-is-the-environmental-impact-of-cryptocurrency; Digiconomist. 2022. Bitcoin Energy Consumption Index. https://digiconomist.net/bitcoin-energy-consumption/, accessed 8 January 2022.

29 O'Callaghan, B. J. and Murdock, E. 2021. "Are We Building Back Better? Evidence from 202 and Pathways to Inclusive Green Recovery Spending". United Nations Environment Programme. March 2021. https://wedocs.unep.org/bitstream/handle/20.500.11822/35281/AWBBB.pdf

30 Council on Foreign Relations. 2021. Global Monetary Policy Tracker. Greenberg Center for Geoeconomic Studies. https://www.cfr.org/global/global-monetary-policy-tracker/p37726

31 White, A. 2021. "'Zombie' firms kept alive by Covid-19 bailouts, EU official says". Bloomberg. 24 February 2021. https://www.bloomberg.com/news/articles/2021-02-24/-zombie-firms-kept-alive-by-covid-19-bailouts-eu-official-says

32 Parry, I., Black, S. and Vernon, N. 2021. "Still not getting energy prices right: A global and country update of fossil fuel subsidies". IMF Working Paper No. 2021/236. 24 September 2021. https://www.imf.org/en/Publications/WP/Issues/2021/09/23/Still-Not-Getting-Energy-Prices-Right-A-Global-and-Country-Update-of-Fossil-Fuel-Subsidies-466004

33 OECD and IEA. 2021. "Update on recent progress in reform of inefficient fossil-fuel subsidies that encourage wasteful consumption 2021". Contribution by the Organisation for Economic Co-operation and Development (OECD) and the International Energy Agency (IEA) to G20 Environment, Climate and Energy Ministers, in consultation with the Organization of Petroleum Exporting Countries (OPEC). Climate and Energy Joint Ministerial Meeting. Naples. 23 July 2021. https://www.oecd.org/g20/topics/climate-sustainability-and-energy/OECD-IEA-G20-Fossil-Fuel-Subsidies-Reform-Update-2021.pdf

34 Clark, A. 2021. "Energy crisis sets stage for record global carbon emissions". Bloomberg. 8 October 2021. https://www.bloomberg.com/news/articles/2021-10-08/energy-crisis-sets-stage-for-record-global-carbon-emissions

35 Brower, D. 2021. "COP26: oil price soars even as the world turns against fossil fuels". Financial Times. 4 November 2021. https://www.ft.com/content/37947e4a-71a1-4c0e-919b-1e3d55ee19ea

36 Egan, M. and Nilsen, E. 2021. "House committee intends to subpoena fossil fuel companies for documents about climate disinformation". CNN. 29 October 2021. https://edition.cnn.com/2021/10/28/politics/fossil-fuel-oversight-hearing-climate/index.html

37 Egan, M. 2021. "Undercover Exxon video reveals an anti-climate campaign". CNN Business. 1 July 2021. https://edition.cnn.com/2021/07/01/business/exxon-tape-video-keith-mccoy/index.html

38 OECD . 2021. Carbon Pricing in Times of COVID-19: What Has Changed in G20 Economies? Paris: OECD. https://www.oecd.org/tax/tax-policy/carbon-pricing-in-times-of-covid-19-what-has-changed-in-g20-economies.htm; World Bank. 2021. Carbon Pricing Dashboard. https://carbonpricingdashboard.worldbank.org/, accessed on 12 December 2021.

39 Dai, R., Duan, R., Liang, H. and Ng, L. 2021. "Outsourcing climate change". European Corporate Governance Institute. Finance Working Paper Number 723/2021. https://ecgi.global/sites/default/files/working_papers/documents/daiduanliangngfinal.pdf

40 Brenton, P. and Chemutai, V. 2021. "The Trade and Climate Change Nexus: The Urgency and Opportunities for Developing Countries". World Bank. https://openknowledge.worldbank.org/handle/10986/36294

41 Zurich Insurance. 2021. "Climate change's forgotten risks". 2 March 2021. https://www.zurich.com/en/knowledge/topics/global-risks/climate-change-forgotten-risks

42 Dunz, N., Naqvi, A. and Monasterolo, I. 2021. "Climate sentiments, transition risk, and financial stability in a stock-flow consistent model". Journal of Financial Stability, Vol. 54. June 2021. https://www.sciencedirect.com/science/article/abs/pii/S1572308921000322?via%3Dihub

43 Bolton, P. and Kacperczyk, M. 2021. "Global pricing of carbon-transition risk". National Bureau of Economic Research Working Paper 28510. February 2021. https://www.nber.org/system/files/working_papers/w28510/w28510.pdf

44 IRENA (International Renewable Energy Agency). 2020. Measuring the Socio-economics of Transition: Focus on Jobs. IRENA. Abu Dhabi. 2020. https://www.irena.org/-/media/Files/IRENA/Agency/Publication/2020/Feb/IRENA_Transition_jobs_2020.pdf

45 Kramer, A.R. 2017. "The myth of 'Stranded Assets' in climate protection". Institute for Advanced Sustainability Studies blog post. Potsdam. 8 December 2017. https://www.iass-potsdam.de/en/node/5572?utm_source=newsletter&utm_medium=email&utm_content=2019-09-08&utm_campaign=greenbuzz

46 Basel Committee on Banking Supervision. 2021. Climate-Related Risk Drivers and Their Transmission Channels. Bank for International Settlements. April 2021. https://www.bis.org/bcbs/publ/d517.pdf

47 Siyobi, B. 2021. "Stranded assets: The nexus between extractives, climate, & the circular economy within the African extractives sectors". South African Institute of International Affairs. June 2021. https://media.africaportal.org/documents/Policy-Insights-112-siyobi.pdf

48 European Agency for Safety and Health at Work. 2021. "Workers' safety and health in green jobs". https://osha.europa.eu/en/emerging-risks/green-jobs; O'Connor, S. 2021. "Not all green jobs are safe and clean". Financial Times. 26 October 2021. https://www.ft.com/content/111f9600-f440-47fb-882f-4a5e3c96fae2

49 The Economist. 2021. "Those who worry about CO2 should worry about methane, too". The Economist. 31 March 2021 Edition. https://www.economist.com/science-and-technology/2021/04/03/those-who-worry-about-co2-should-worry-about-methane-too

50 Swiss Re. 2021. The Economics of Climate Change. Op. cit.

51 Cursino, M. and Faulkner, D. 2021. "COP26: China and India must explain themselves, says Sharma". BBC. 14 November 2021. https://www.bbc.com/news/uk-59280241

52 Greenhalgh, K. 2021. "Nigerian government retains focus on gas-based transition". HIS Markit. 16 August 2021. https://ihsmarkit.com/research-analysis/nigerian-government-retains-focus-on-gasbased-transition.html

53 Brenton, P. and Chemutai, V. 2021. The Trade and Climate Change Nexus: The Urgency and Opportunities for Developing Countries. World Bank. https://openknowledge.worldbank.org/handle/10986/36294

54 Duwe, S. and Humbs, C. "Ausgebremst: Windkraft in der Krise". Kontraste, ARD (German Television). 15 July 2021. https://www.rbb-online.de/kontraste/archiv/kontraste-vom-15-07-2021/ausgebremst-windkraft-in-der-krise.html

55 SENEC. 2021. "Einspeisevergütung für PV Anlagen – lohnt sich das noch?". SENEC GmbH. Leipzig. https://senec.com/de/photovoltaikanlage/einspeiseverguetung

56 Deutsche Welle. 2021. "EU states spilt on classifying nuclear energy as 'green'". Deutsche Welle. 11 November 2021. https://www.dw.com/en/eu-states-split-on-classifying-nuclear-energy-as-green/a-59792406

57 Hellstern, T., Henderson, K., Kane, S. and Rogers, M. 2021. "Innovating to net zero: An executive's guide to climate technology". McKinsey. 28 October 2021. https://www.mckinsey.com/business-functions/sustainability/our-insights/innovating-to-net-zero-an-executives-guide-to-climate-technology

58 Reynolds, J.L. 2019. "Solar geoengineering to reduce climate change: a review of governance proposals". Proceedings of the Royal Society A. 475:20190255. https://royalsocietypublishing.org/doi/10.1098/rspa.2019.0255

59 Jones, A.C., Hawcroft, M.K., Haywood, J.M., Jones, A., Guo, X. and Moore, J.C. 2018. "Regional climate impacts of stabilizing global warming at 1.5 K using solar geoengineering". Earth's Future 6 (2): 230–251. https://agupubs.onlinelibrary.wiley.com/doi/full/10.1002/2017EF000720

60 Trisos, Ch.H., Amatulli, G., Gurevitch, J., Robock, A., Xia, L. and Zambri, B. 2018. "Potentially dangerous consequences for biodiversity of solar geoengineering implementation and termination". Nature Ecology & Evolution. 2, 475–482. https://www.nature.com/articles/s41559-017-0431-0

61 Goswani, A. 2021. "Why geoengineering is still a dangerous, techno-utopian dream". Downtoearth.org. 30 December 2021. https://www.downtoearth.org.in/blog/climate-change/why-geoengineering-is-still-a-dangerous-techno-utopian-dream-74828; UNEP (United Nations Environment Programme). 2021. Net-zero asset owner alliance back call to scale-up carbon removal from atmosphere. United Nations Environment Programme. 23 September 2021. https://www.unepfi.org/news/industries/investment/net-zero-asset-owner-alliance-backs-call-to-scale-up-carbon-removal-from-atmosphere/

62 UNEP (United Nations Environment Programme). 2021. The Net in Net Zero: The Role of Negative Emissions in Achieving Climate Alignment for Asset Owners. UNEP and PRI. September 2021. https://www.unepfi.org/publications/the-role-of-negative-emissions-in-achieving-climate-alignment-for-asset-owners/

63 Kusnetz, N. 2021. "Fossil fuel companies are quietly scoring big money for their preferred climate solution: Carbon capture and storage". Inside Climate News. 17 August 2021. https://insideclimatenews.org/news/17082021/carbon-capture-storage-fossil-fuel-companies-climate/

64 Fairs, M. 2021. "Carbon washing is the new greenwashing". Dezeen. 31 July 2021. https://www.dezeen.com/2021/07/31/carbon-washing-greenwashing-opinion/

65 Heck, V., Gerten, D., Lucht, W. and Popp, A. 2018. "Biomass-based negative emissions difficult to reconcile with planetary boundaries". Nature Climate Change. 8, 151–155. https://www.nature.com/articles/s41558-017-0064-y; O'Leary, S. and Hunkler, B. 2021. "Carbon capture, use, and sequestration (CCUS) would decarbonize the electric system . . . in the worst possible way". Ohio River Valley Institute. https://ohiorivervalleyinstitute.org/wp-content/uploads/2021/10/CCUS-Report-FINAL-3.pdf

66 IRENA. 2020. Op. cit.

67 Jones, C. 2020. "Was hyperglobalisation an anomaly?". Financial Times. 17 November 2020. https://www.ft.com/content/a89f5911-5cba-4d62-8746-5213303a92ec; OECD. 2021. "What happened to jobs at high risk of automation?" OECD. January 2021. https://www.oecd.org/future-of-work/reports-and-data/what-happened-to-jobs-at-high-risk-of-automation-2021.pdf; Rodrik, D. 2019. "Globalization's wrong turn: And how it hurt America". Foreign Affairs. July/August 2019. https://www.foreignaffairs.com/articles/united-states/2019-06-11/globalizations-wrong-turn

68 UNCTAD (United Nations Conference on Trade and Development). 2021. Technology and Innovation Report 2021: Catching Technological Waves – Innovation with Equity. Geneva: UN. https://unctad.org/system/files/official-document/tir2020_en.pdf

69 UNCTAD. 2020. "Developing countries pay environmental cost of electric car batteries". 22 July 2020. https://unctad.org/news/developing-countries-pay-environmental-cost-electric-car-batteries

70 OECD. 2021. FDI Flows. https://data.oecd.org/fdi/fdi-flows.htm, accessed 15 December 2021.

71 OECD. 2021. Climate Finance Provided and Mobilised by Developed Countries: Aggregate Trends Updated with 2019 Data. OECD. 17 September 2021. https://www.oecd.org/env/climate-finance-provided-and-mobilised-by-developed-countries-aggregate-trends-updated-with-2019-data-03590fb7-en.htm

72 Zurich Insurance. 2021. "Climate change's forgotten risks". 2 March 2021. https://www.zurich.com/en/knowledge/topics/global-risks/climate-change-forgotten-risks

73 Van der Ploeg, F. and Rezai, A. 2020. "Stranded assets in the transition to a carbon-free economy". Annual Review of Resource Economics 12: 281–298. https://www.annualreviews.org/doi/10.1146/annurev-resource-110519-040938

74 Basel Committee on Banking Supervision. 2021. Climate-Related Risk Drivers and Their transmission Channels. Bank for International Settlements. April 2021. https://www.bis.org/bcbs/publ/d517.pdf

75 Dunz, N., Naqvi, A. and Monasterolo, I. 2021. "Climate sentiments, transition risk, and financial stability in a stock-flow consistent model". Journal of Financial Stability 54. June 2021. https://www.sciencedirect.com/science/article/abs/pii/S1572308921000322?via%3Dihub

76 Timperley, J. 2021. "The truth behind corporate climate pledges". The Guardian. 26 July 2021. https://www.theguardian.com/environment/2021/jul/26/climate-crisis-green-light

77 Court of The Hague. 2021. Op cit.

78 Bailey, R., Yeo, J., Jiang, L. and Ferguson, A. 2020. ESG as a Workforce Strategy: Engaging Today's Employees and Attracting Tomorrow's Talent. Marsh McLennan. https://www.marshmclennan.com/insights/publications/2020/may/esg-as-a-workforce-strategy.html

79 Dominish, E., Florin, N. and Teske, S. 2019. Responsible Minerals Sourcing for Renewable Energy. Report prepared for Earthworks by the Institute for Sustainable Futures, University of Technology Sydney. https://earthworks.org/assets/uploads/2019/04/MCEC_UTS_Report_lowres-1.pdf

CHAPTER 3

Digital Dependencies and Cyber Vulnerabilities

435%

increase in ransomware in 2020

3 million

gap in cyber professionals needed worldwide

US$

800 billion

estimated growth in value of digital commerce by 2024

95%

cybersecurity issues traced to human error

GETTY/THOMAS TRUTSCHEL

Digital distress

Governments, societies and companies increasingly rely on technology to manage everything from public services to business processes, even routine grocery shopping.[1] Converging technological platforms, tools and interfaces connected via an internet that is rapidly shifting to a more decentralized version 3.0 are at once creating a more complex cyberthreat landscape and a growing number of critical failure points. As society continues to migrate into the digital world, the threat of cybercrime looms large, routinely costing organizations tens—even hundreds—of millions of dollars. The costs are not just financial: critical infrastructure, societal cohesion and mental well-being are also in jeopardy.

Digital everything

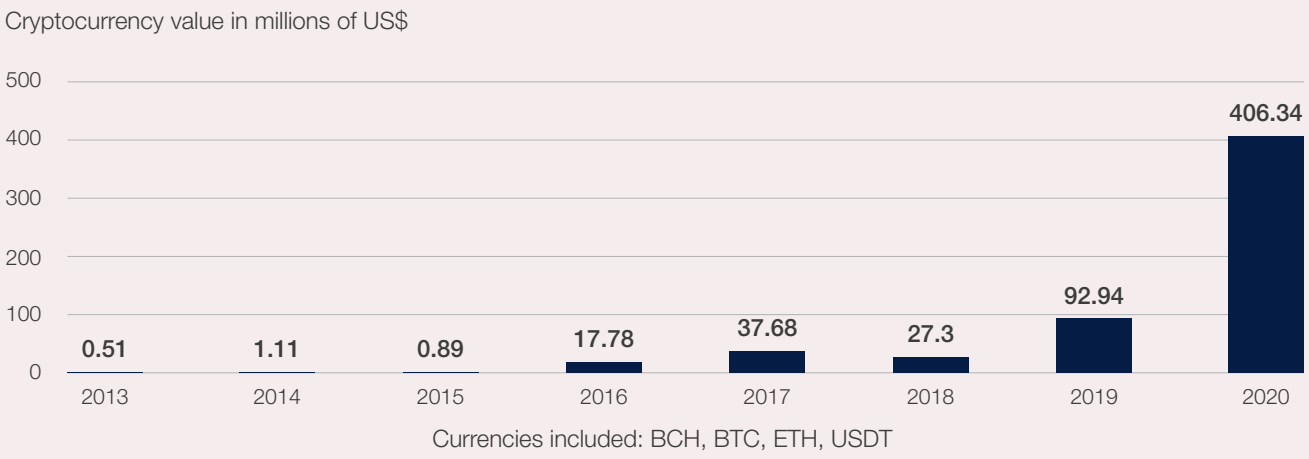
Growing dependency on digital systems over the last 20 years has drastically shifted how many societies function.[2] The COVID-19-induced shift to remote work has accelerated the adoption of platforms and devices that allow sensitive data to be shared with third parties—cloud service providers, data aggregators, application programming interfaces (APIs) and other technology-related intermediaries.[3] These systems, while powerful tools for data and processing, attach an additional layer of dependency on service providers. Remote work has also moved digital exchanges from office networks to residential ones, which have a greater variety of connected devices with less protection against cyber intrusion. In parallel, the appetite for capabilities predicated upon using multiple technologies working in concert—including artificial intelligence (AI), Internet of Things (IoT)/ Internet of Robotic Things–enabled devices, edge computing, blockchain and 5G—is only growing.[4] While these capabilities afford tremendous opportunities for businesses and societies to use technology in ways that can dramatically improve efficiency, quality and productivity, these same capabilities also expose users to elevated and more pernicious forms of digital and cyber risk.

In the future, the interconnectedness and convergence of these digital tools will continue to increase as society embraces the next version of the internet built upon blockchain technology. One manifestation of this migration will be the metaverse: a network of 3D virtual spaces, enabled by cryptocurrencies and non-fungible tokens (NFTs) among other technologies, with unprecedented socio-economic interoperability and immersive virtual reality experiences.[5] Users will be required to navigate security vulnerabilities inherent in both increased dependency on and growing fragmentation in these types of complex technologies often characterized by decentralization and lack of structured guardrails or sophisticated onboarding infrastructure.

GETTY/FILIPPOBACCI

FIGURE 3.1

Total Cryptocurrency Value Received by Ransomware Addresses, 2013-2020



Source: Based on Chainanalysis. Ransomware 2021: Critical Mid-Year Update. Insights blog. https://blog.chainalysis.com/reports/ransomware-update-may-2021

Cyber vulnerabilities

In the context of widespread dependency on increasingly complex digital systems, growing cyberthreats are outpacing societies' ability to effectively prevent and manage them. For example, the digitalization of physical supply chains creates new vulnerabilities because those supply chains rely on technology providers and other third parties, which are also exposed to similar, potentially contagious, threats.[6] In December 2021, just one week after discovering a critical security flaw in a widely used software library (Log4j), more than 100 attempts at exploiting the vulnerability were detected every minute, illustrating how free access coding can spread vulnerabilities widely.[7] Information technology (IT) monitoring and management software also illustrate the potential for contagious exposure, which can break through the defences of critical cybersecurity supply chains, as shown by the Solar Winds Orion attack that occurred in late 2020.[8] While a state-based institution with highly sophisticated capabilities probably lodged this attack, other criminal organizations will certainly attempt to replicate this approach.[9] At the same time, older vulnerabilities persist with many organizations still relying on outdated systems or technologies.

Malicious activity is proliferating, in part because of the growing vulnerabilities—but also because there are few barriers to entry for participants in the ransomware industry and little risk of extradition, prosecution or sanction.[10] Malware increased by 358% in 2020, while ransomware increased by 435%,[11] with a four-fold rise in the total cryptocurrency value received by ransomware addresses (see Figure 3.1).[12] "Ransomware as a service" allows even non-technical criminals to execute attacks, a trend that might intensify with the advent of artificial intelligence (AI)-powered malware.[13] In fact, profit-seeking groups of cyber mercenaries stand ready to provide access to sophisticated cyber-intrusion tools to facilitate such attacks. Furthermore, cryptocurrencies have also allowed cybercriminals to collect payments with an only modest risk of detection or monetary clawback.[14]

Attacks themselves are also becoming more aggressive and widespread.[15] Cyberthreat actors using ransomware are leveraging tougher pressure tactics as well as going after more vulnerable targets, impacting public utilities, healthcare systems and data-rich companies.[16] For example, before it disbanded, DarkSide—the group accused of being responsible for the Colonial Pipeline attack—offered a suite of services ("triple" or "quadruple" extortion)

REUTERS/JIM YOUNG

to clients beyond simply encrypting files; these included data leaks and distributed denial-of-service (DDoS) attacks. Hacker groups will also contact victims' clients or partners to get them to urge the victims to pay ransoms. Among the services offered is the collection of top executive information for blackmail.[17]

Sophisticated cyber tools are also allowing cyberthreat actors to attack targets of choice more efficiently, rather than settling for targets of opportunity, highlighting the potential to carry out more goal-oriented attacks that could lead to even higher financial, societal and reputational damage in the future. Increasingly sophisticated use of spyware technologies, for example, has allowed for targeted attacks against journalists and civil rights activists across geographies—spurring a wave of political and industrial blowback in the form of government sanctions and lawsuits.[18] The ability to tailor attacks at will includes timing them for when cybersecurity teams and leadership could be distracted by other priorities, such as during peak COVID-19 outbreaks or a natural disaster. Cyberthreat actors are also accessing higher-quality and more sensitive information from victims. And deepfake technology is allowing cyberthreat actors to improve social engineering ploys, proliferate disinformation and wreak societal havoc, especially at times of high volatility.[19]

Global Risks Perception Survey (GRPS) respondents reflect these trends, ranking "cybersecurity failure" among the top-10 risks that have worsened most since the start of the COVID-19 crisis. Moreover, 85% of the Cybersecurity Leadership Community of the World Economic Forum have stressed that ransomware is becoming a dangerously growing threat and presents a major concern for public safety.[20] At a regional level, "cybersecurity failure" ranks as a top-five risk in East Asia and the Pacific as well as in Europe, while four countries—Australia, Great Britain, Ireland and New Zealand—ranked it as the number one risk. Many small, highly digitalized economies—such as Denmark, Israel, Japan, Taiwan (China), Singapore and the United Arab Emirates—also ranked the risk as a top-five concern.

Already-stretched IT and cybersecurity professionals are under an increasing burden, not only because of the expansion of remote work but also because of the growing complexity of regulations for data and privacy, even though such regulations are critical to ensuring public trust in digital systems.[21] There is an undersupply of

"Cybersecurity failure" is one of the risks that worsened the most through COVID-19

cyber professionals—a gap of more than 3 million worldwide[22]—who can provide cyber leadership, test and secure systems, and train people in digital hygiene.[23] As with other key commodities, a continued lack of cybersecurity professionals could ultimately hamper economic growth,[24] although new initiatives to "democratize" cybersecurity, for example, by providing free cybersecurity risk management tools, could help fill some of the gaps for small businesses or other institutions.[25]

There are concerns that quantum computing could be powerful enough to break encryption keys—which poses a significant security risk because of the sensitivity and criticality of the financial, personal and other data protected by these keys. The emergence of the metaverse could also expand the attack surface for malicious actors by creating more entry points for malware and data breaches.[26] As the value of digital commerce in the metaverse grows in scope and scale—by some estimates projected to be over US$800 billion by 2024—these types of attacks will grow in frequency and aggression.[27] The myriad forms of digital property such as NFT art collections and digital real estate could further entice criminal activity.

For governments attempting to prevent cybersecurity failures, patchwork enforcement mechanisms across jurisdictions continue to hamper efforts to control cybercrime.[28] Geopolitical rifts hinder potential cross-border collaboration, with some governments unwilling or unable to regulate cyber intrusions that originate inside and impact outside their borders. Unsurprisingly, given the geopolitical tensions around digital sovereignty, according to GRPS respondents, "cross-border cyberattacks and misinformation" and "artificial intelligence" were among the areas with the least "established" or "effective" international risk mitigation efforts.

Companies must also act ahead of new regulatory shifts, as the political undercurrents/geopolitical tensions between various countries might impact cross-border data flows. This might mean moving data processing to jurisdictions that might allow for better customer protection around data privacy issues.[29]

Consequences

Often-repeated examples of past cyber intrusions are worth re-examination, as these cases demonstrate how damaging attacks on large and strategically significant systems—such as banking, hospital, Global Positioning System (GPS) or air traffic control systems—could be.[30] As resources are increasingly digitized, notable as well is the heightened risk of cyber espionage attacks that typically target intellectual property and result in high developmental and reputational costs to both private and public sector organizations.[31]

The interaction between digitalization and growing cyberthreats carries intangible consequences as well. The growth of deepfakes and "disinformation-for-hire" is likely to deepen mistrust between societies, business and government.[32] For example, deepfakes could be used to sway elections or political outcomes.[33] More concretely, in one recent case, cybercriminals cloned the voice of a company director to authorize the transfer of US$35 million to fraudulent accounts.[34] There is also a booming market for services designed to manipulate public opinion in favour of clients, public or private, or to damage rivals.[35] Fraud, too, will become easier and therefore more frequent with banking, health and civic processes going remote.

Patchwork enforcement mechanisms continue to hamper efforts to control cybercrime

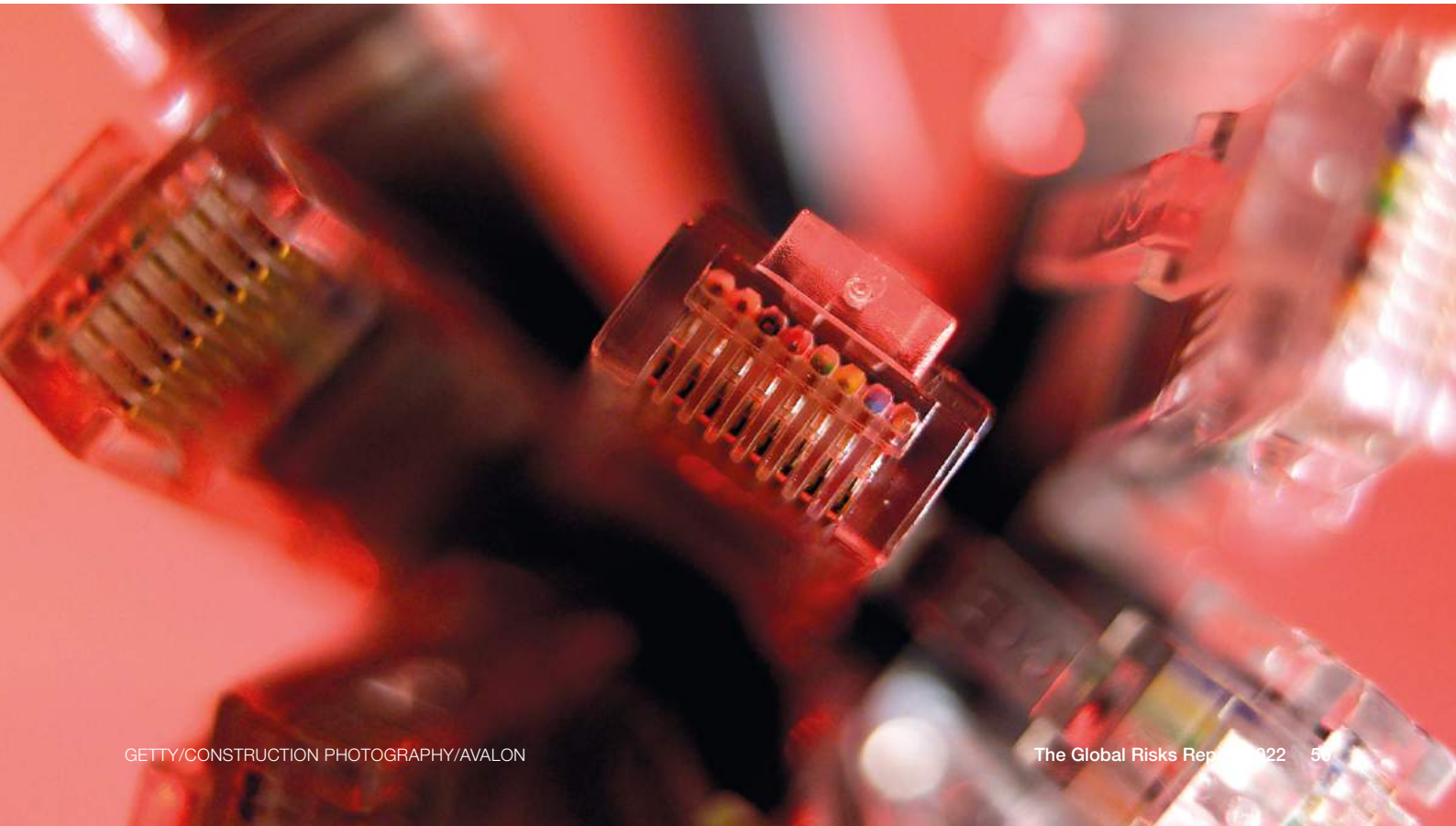
In 2021, UK internet banking fraud rose by 117% in volume and 43% in value compared with 2020 levels, as people spent more time shopping online.[36] Digital safety overall—from health misinformation and extremism to child exploitation—faces new challenges with unexperienced and more vulnerable populations coming online.[37]

Even in the best-case scenario of aggressive digital threat defences, there will be significant increases in the cost of operations for all stakeholders. This could be particularly challenging for small- or medium-sized businesses that might spend 4% or more of their operational budget on security, compared to larger organizations that might spend closer to 1–2%.[38] Indeed, amid the rising frequency and severity of ransomware claims, cyber insurance pricing in the United States rose by 96% in the third quarter of 2021, marking the most significant increase since 2015 and a 204% year-over-year increase.[39] Respondents to the GRPS indicate a long-term concern with these developments, with "adverse tech advances" appearing as a top-10 risk over a 5-to-10-year horizon.

Cyberthreats also continue to drive states apart, with governments following increasingly unilateral paths to control risks. As attacks become more severe and broadly impactful, already-sharp tensions between governments impacted by cybercrime and governments complicit in their commission will rise as cybersecurity becomes another wedge for divergence, rather than cooperation, among nation states.[40] Particularly in an era of rising tensions between superpowers, cyberattacks are another battlefront in which escalation is a key risk (see Chapter 1).[41] If cyberthreats continue without mitigation, governments will continue to retaliate against perpetrators (actual or perceived), leading to open cyberwarfare, further disruption for societies and loss of trust in governments' ability to act as digital stewards.

Digital security divides: Consequences for people

Among the most vulnerable are those who are only now coming online or will soon do so. Around 40% of the world's population is not yet connected to the internet.[42] These individuals are already facing inequalities in digital security, which will only widen with the advent of internet 3.0 and the metaverse.[43] Within digitally advanced societies, vulnerable populations are also often more digitally at risk: for example, a recent study finds that low-income residents of San Francisco—

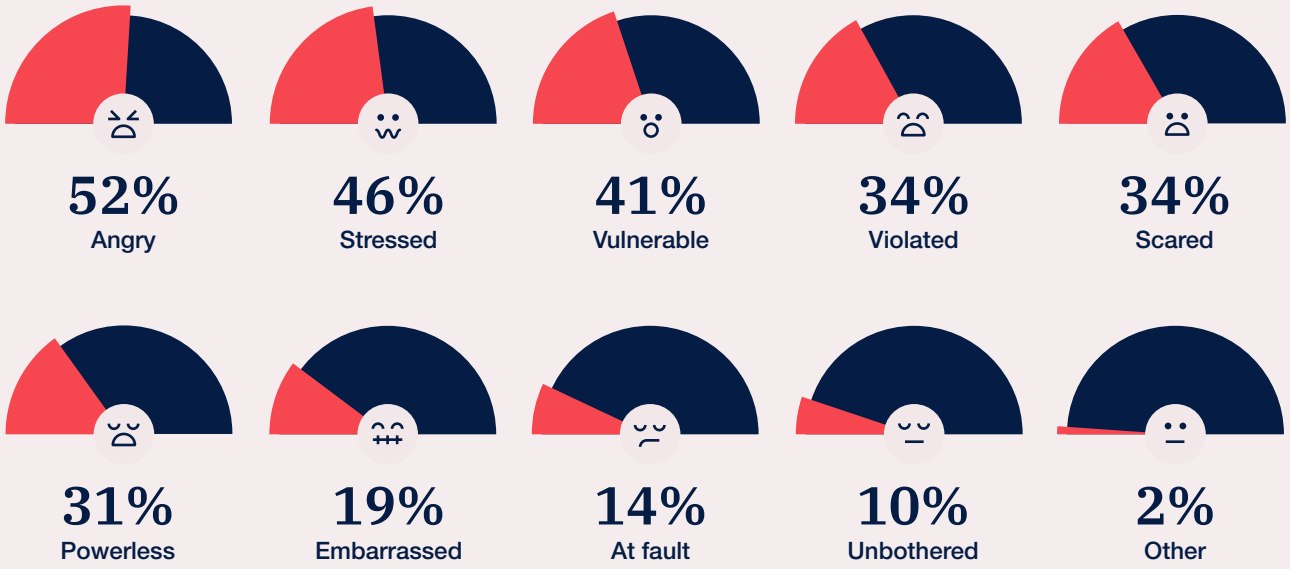


GETTY/CONSTRUCTION PHOTOGRAPHY/AVALON

FIGURE 3.2

Emotions Experienced after Detecting Unauthorized Access

Global total of those who detected unauthorized access in past 12 months



Source: NortonLifeLock Inc. 2021. "2021 Norton Cyber Safety Insights Report: Global Results". Norton and The Harris Poll. May 2021. https://now.symassets.com/content/dam/norton/campaign/NortonReport/2021/2021_NortonLifeLock_Cyber_Safety_Insights_Report_Global_Results.pdf

the cultural heart of Silicon Valley—are more likely than wealthier residents to be cybercrime victims.[44] In other situations, obligatory digital identity markers could introduce new risks for citizens, particularly evident in the growing risk that deepfakes could compromise biometric authentication.[45]

Individuals will increasingly experience anxiety as control over their data becomes more precarious and they are subjected to personal attacks, fraud, cyberbullying and stalking (see Figure 3.2).[46] A perceived lack of agency could also lead to apathy in taking responsibility for securing one's own digital footprint, as evinced by the continued market dominance of instant messenger applications plagued by privacy controversies.[47] Even with more widespread "reject all" options on websites intended to simplify personal data privacy, there are drawbacks and caveats—such as limiting functionality and other options. Importantly, these features are just a tiny part of the larger privacy equation. Websites are still littered with tracking pixels and third-party scripts that remain powerful ways to fingerprint online behaviours.[48]

Overreaching or underdelivering: Consequences for governments

Government at all levels faces mounting responsibilities and many are struggling to uphold their end of the digital social contract: securing critical infrastructure; addressing threats to "epistemic security" from disinformation; protecting the integrity of civic processes and public services; legislating against cybercrime; training and educating populaces around cyber literacy; regulating digital service providers; and ensuring the availability of resources, such as rare-earth minerals, for the digital economy. The necessary oversight could lead to overreach as governments move to shut down systems, erect higher digital barriers or embark on digital colonization (by monopolizing digital systems) for geopolitical ends.[49] While such actions might carry the ostensible goal of reducing

attacks and disruption, these policies could quickly become a vehicle for oppression. Already suffering from a loss in public trust as a result of the COVID-19 crisis, governments may face further societal anger if they are unable to both keep up with the shifting threat landscape and responsibly manage these challenges.

Pay, protect or perish: Consequences for businesses

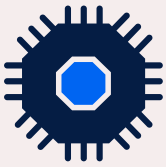
As cyberthreats continue to grow, insuring against such risks will become increasingly precarious, with insurers themselves facing retaliatory attacks for attempting to curb ransomware payments.[50] Thus, when an attack occurs, businesses will either be forced to pay increasingly high ransoms or suffer the reputational, financial, regulatory and legal consequences of cyberattacks. As previous incursions (like SolarWinds) have demonstrated, exposure to vendors and supply chain partners must also be assessed and managed. The impact of disruptive cyberattacks could be financially devastating for businesses that fail to invest in protections for their digital infrastructure, particularly in a scenario in which governments begin prohibiting ransom payments or penalizing poor cybersecurity practices.[51] Furthermore, as environmental, social and governance (ESG) concerns come increasingly into focus (see Chapter 2), businesses that fail to demonstrate strong corporate governance around cybersecurity—such as by implementing robust systems and process oversight protocols, and by practicing accountability and transparency in the event of a breach—could suffer reputational harm in the eyes of ESG-focused investors.

Businesses also operate in a world in which 95% of cybersecurity issues can be traced to human error,[52] and where insider threats (intentional or accidental) represent 43% of all breaches.[53] Some companies will inevitably move to greater segmentation of digital systems to better account for insider risk. Companies could begin or continue to lock up key data as a result of the cybersecurity issues. Workforce efficiency, too, could suffer if accessing data and information is less seamless.

Shocks to reflect upon

NotPetya 2.0

What if an attack that is even more wide-ranging and costly than NotPetya—with the ability to self-propagate and even mutate to avoid preventative controls—created cascading lockups of systemically important businesses, bankrupting organizations, disrupting services and unwinding the digital transformation efforts made over the past years?



Sovereignty slips

What if the shifts towards privately held IT infrastructure as well as cryptocurrency and decentralized finance undermine governments' control over data, processes and financial systems?

Undetected disruption

What if subtle changes in health, banking or other data go undetected for years, but carry significant consequences for premature death, loss of funds or other significant consequences over time? How can cyber espionage compromise return on R&D investment and competitiveness in the future?

Towards greater cyber resilience

As our reliance on digital technologies grows and Internet 3.0 becomes reality, efforts aimed at building norms and defining rules of behaviour for all stakeholders in cyberspace are intensifying. While multistakeholder international dialogues can help strengthen links between actors operating in the digital security realm, cooperation between organizations could unlock best practices that can be replicated across industries and economies. Initiatives should focus on emerging technologies, such as blockchain, quantum and artificial intelligence, as well as the modes of digital exchange they facilitate, like the metaverse. Leaders must remain attentive to perennial concerns like cybercrime and ransomware attacks as well. At the organizational level, upskilling leaders on cybersecurity issues and elevating emerging cyber risks to board-level conversations will strengthen cyber-resilience. In a deeply connected society, digital trust is the currency that facilitates future innovation and prosperity. Trustworthy technologies, in turn, represent the foundation on which the scaffolding of a fair and cohesive society is built. Unless we act to improve digital trust with intentional and persistent trust-building initiatives, the digital world will continue to drift towards fragmentation and the promise of one of the most dynamic eras of human progress may be lost.

REUTERS/MAXIM SHEMETOV

Endnotes

1 World Economic Forum, in partnership with Marsh & McLennan Companies, SK Group and Zurich Insurance Group. 2021. The Global Risks Report 2021. Insight Report. Chapter 2 Error 404. Geneva: World Economic Forum. January 2021. https://www.weforum.org/reports/the-global-risks-report-2021

2 World Economic Forum, in partnership with Marsh & McLennan Companies and Zurich Insurance Group. 2020. The Global Risks Report 2020. Insight Report. Chapter 5 Wild Wide Web. Geneva: World Economic Forum. January 2020. https://www.weforum.org/reports/the-global-risks-report-2020

3 Check Point Software Technologies Ltd. 2021. The Biggest Cloud Security Challenges of 2021. https://pages.checkpoint.com/2020-cloud-security-report.html?utm_term=cyber-hub; Kent, J. 2020. "APIs are the next frontier in cybercrime". Security. 3 September 2020. https://www.securitymagazine.com/articles/93239-apis-are-the-next-frontier-in-cybercrime

4 Hoster, B. and Sequeira, T. 2021. Harnessing Technology Convergence: Lessons from Smart Manufacturers. Marsh McLennan. https://www.marshmclennan.com/insights/publications/2021/may/harnessing-technology-convergence.html

5 Allyn, B. 2021. "People are talking about Web3. Is it the Internet of the future or just a buzzword?" National Public Radio. 21 November 2021. https://www.npr.org/2021/11/21/1056988346/web3-internet-jargon-or-future-vision; Clark, P.A. 2021. "The metaverse has already arrived. Here's what that actually means". Time. 15 November 2021. https://time.com/6116826/what-is-the-metaverse/; Robertson, A. and Peters, J. 2021. "What is the metaverse, and do I have to care?" The Verge. 4 October 2021. https://www.theverge.com/22701104/metaverse-explained-fortnite-roblox-facebook-horizon

6 World Economic Forum, in partnership with Marsh & McLennan Companies, SK Group and Zurich Insurance Group. 2021. The Global Risks Report 2021. Insight Report. Chapter 5 Imperfect Markets. Geneva: World Economic Forum. January 2021. https://www.weforum.org/reports/the-global-risks-report-2021

7 Korn, J. 2021. "The Log4j security flaw could impact the entire internet. Here's what you should know". CNN. 15 December 2021. https://edition.cnn.com/2021/12/15/tech/log4j-vulnerability/index.html

8 Reuters Staff. 2021. "SolarWinds hack was 'largest and most sophisticated attack' ever: Microsoft president". Reuters. 15 February 2021. https://www.reuters.com/article/us-cyber-solarwinds-microsoft-idUSKBN2AF03R

9 Burke, S. 2021. "Cyber-crime learnings and predictions for 2021". Counter Terror Business. 15 January 2021. https://counterterrorbusiness.com/features/cyber-crime-learnings-and-predictions-2021

10 Coveware. 2021. "Ransomware attackers down shift to 'Mid-Game' hunting in Q3 2021". 21 October 2021. https://www.coveware.com/blog/2021/10/20/ransomware-attacks-continue-as-pressure-mounts

11 Help Net Security. 2021. "Malware increased by 358% in 2020". Help Net Security. 17 February 2021. https://www.helpnetsecurity.com/2021/02/17/malware-2020/

12 Chainalysis Team. 2021. "Ransomware 2021: Critical mid-year update". Insights. 14 May 2021. https://blog.chainalysis.com/reports/ransomware-update-may-2021

13 Sharton, B.R. 2021. "Ransomware attacks are spiking. Is your company prepared?" Harvard Business Review. 20 May 2021. https://hbr.org/2021/05/ransomware-attacks-are-spiking-is-your-company-prepared; Steib, M. 2021. "What's driving the surge in ransomware attacks?" New York Magazine Intelligencer. 7 September 2021. https://nymag.com/intelligencer/article/ransomware-attacks-2021.html; Pupillo, L. et al. 2021. "Artificial Intelligence and Cyber Security." CEPS Task Force. May 2021. https://www.ceps.eu/wp-content/uploads/2021/05/CEPS-TFR-Artificial-Intelligence-and-Cybersecurity.pdf

14 Rosenzweig, P. 2021. "There's a better way to stop ransomware attacks". New York Times (Guest Essay). 31 August 2021. https://www.nytimes.com/2021/08/31/opinion/ransomware-bitcoin-cybersecurity.html

15 Davis, E. and Mee, P. 2021. Growing Cyber Threat Demands a United Response. Marsh McLennan. https://www.marshmclennan.com/insights/publications/2021/october/growing-cyber-threat-demands-a-united-response.html

16 Accenture. 2021. Threats Unmasked: 2021 Cyber Threat Intelligence Report. 2021. https://www.accenture.com/_acnmedia/PDF-158/Accenture-2021-Cyber-Threat-Intelligence-Report.pdf; BBC. 2021. "Hacker tries to poison water supply of Florida city". BBC. 8 February 2021. https://www.bbc.com/news/world-us-canada-55989843; European Insurance and Occupational Pensions Authority. 2021. "Cyber risks: what is the impact on the insurance industry?" 15 October 2021. https://www.eiopa.europa.eu/media/feature-article/cyber-risks-what-impact-insurance-industry_en; Poulsen, K., McMillan, R. and Evans, M. 2021. "A hospital hit by hackers, a baby in distress: The case of the first alleged ransomware death". Wall Street Journal. 30 September 2021. https://www.wsj.com/articles/ransomware-hackers-hospital-first-alleged-death-11633008116; Sganga, N., Herridge, C. and Bidar, M. 2021. "Foreign hacking group targets hospitals, clinics with ransomware attacks, says new report". CBS News. 7 October 2021. https://www.cbsnews.com/news/cyberattacks-ransomware-hacking-hospitals-target-foreign-groups/

17 Accenture. 2021. Op. cit.

18 2021. "Apple sues Israeli firm NSO Group over spyware". Al Jazeera. 23 November 2021. https://www.aljazeera.com/news/2021/11/23/apple-sues-israeli-firm-nso-group-over-spyware

19 Collins, A. and Ebrahimi, T. 2021. "Risk governance and the rise of deepfakes". EPFL International Risk Governance Center. 12 May 2021. https://www.epfl.ch/research/domains/irgc/spotlight-on-risk-series/risk-governance-and-the-rise-of-deepfakes/

20 Cyber Outlook Series virtual workshop on survey results held on 31 March 2021 from Geneva by the Centre for Cybersecurity.

21 Herbert Smith Freehills. 2021. "China's new laws complicate data transfers". 24 August 2021. https://hsfnotes.com/data/2021/08/24/chinas-new-laws-inhibit-data-transfers/

22 Chandrasekhar, C. and Mee, P. 2021. "Why businesses and governments must fight cyber threats together". World Economic Forum Global Agenda. 3 May 2021. https://www.weforum.org/agenda/2021/05/cybersecurity-governments-business/

23 Insight. 2021. Cybersecurity at a Crossroads: The Insight 2021 Report. 4 March 2021. https://www.insight.com/content/dam/insight-web/en_US/pdfs/insight/cybersecurity-at-a-crossroads/cybersecurity-at-a-crossroads--the-insight-2021-report.pdf

24 Cf. Tay, S. 2019. "A serious shortage of cybersecurity experts could cost companies hundreds of millions of dollars". CNBC. 5 March 2019. https://www.cnbc.com/2019/03/06/cybersecurity-expert-shortage-may-cost-companies-hundreds-of-millions.html

25 Bloomberg. 2019. "Coalition Secures $40M in Funding to Democratize Access to Cybersecurity". Press Release. 9 May 2019. https://www.bloomberg.com/press-releases/2019-05-09/coalition-secures-40m-in-funding-to-democratize-access-to-cybersecurity

26 Boyd, C. 2021. "Zuckerberg's Metaverse, and the possible privacy and security concerns". Malwarebytes Labs. 2 November 2021. https://blog.malwarebytes.com/privacy-2/2021/11/zuckerbergs-metaverse-and-the-possible-privacy-and-security-concerns/; Department of Homeland Security. 2021. Post-Quantum Cryptography. https://www.dhs.gov/quantum; Kalmann, A. 2018. "Blog: Cyber Security & the Metaverse". IBC365. 22 June 2018. https://www.ibc.org/blog-cyber-security-and-the-metaverse/2904.article

27 Kanterman M. and Naidu N. 2021 "Metaverse may be $800 billion market, next tech platform". Bloomberg Intelligence. 1 December 2021. https://www.bloomberg.com/professional/blog/metaverse-may-be-800-billion-market-next-tech-platform/

28 Steib. 2021. Op. cit.

29 Murgia M. 2021. "Palantir to reshore all UK data processing from US before regulatory 'tsunami' hits". 17 December 2021. https://www.ft.com/content/76fa6a3f-a818-4e88-be14-b578ae378d7c

30 Pocock, J. and O'Brien, S. 2021. Cyber Risk: The Emerging Cyber Threat to Industrial Control Systems. Lloyd's, CyberCube, and Guy Carpenter. 2021. https://www.marshmclennan.com/content/dam/mmc-web/insights/publications/2021/august/The%20Emerging%20Cyber%20Threat%20to%20Industrial%20Control%20Systems_Final%2016.02.2021.pdf

31 Verizon. 2020. 2020-2021. Cyber-Espionage Report. https://www.verizon.com/business/resources/reports/2020-2021-cyber-espionage-report.pdfx

32 Buckley, J. and Conner, S. 2021. "Cyber Threats: Living with Disruption". Control Risks and AirMic. 12 October 2021. https://www.controlrisks.com/our-thinking/insights/reports/cyber-threats-living-with-disruption

33 See, e.g., CBS News. 2019. "Doctored Nancy Pelosi video highlights threat of "deepfake" tech". 26 May 2019. https://www.cbsnews.com/news/doctored-nancy-pelosi-video-highlights-threat-of-deepfake-tech-2019-05-25/

34 Brewster, T. 2021. "Fraudsters cloned company director's voice in $35 million bank heist, police find". Forbes. 14 October 2021. https://www.forbes.com/sites/thomasbrewster/2021/10/14/huge-bank-fraud-uses-deep-fake-voice-tech-to-steal-millions/?sh=af66cf275591

35 Fisher, M. 2021. "Disinformation for hire, a shadow industry, is quietly booming". The New York Times. 25 July 2021. https://www.nytimes.com/2021/07/25/world/europe/disinformation-social-media.html; Joyce, S., Kashifuddin, M., Nocera, J. and Upton, P. 2021. "The disinformation age has arrived. Are you ready?" PwC. 9 February 2021. https://www.pwc.com/us/en/tech-effect/cybersecurity/corporate-sector-disinformation.html

36 UK Finance. 2021. Fraud — The Facts 2021. https://www.ukfinance.org.uk/system/files/Fraud%20The%20Facts%202021-%20FINAL.pdf

37 Moon Sehat, C. 2021. "Advancing digital safety: A framework to align global action". World Economic Forum. June 2021. https://www3.weforum.org/docs/WEF_Advancing_Digital_Safety_A_Framework_to_Align_Global_Action_2021.pdf; Lalani, F. 2021. "Risks to kids online are growing. Here's what we can do". World Economic Forum. 13 October 2021. https://www.weforum.org/agenda/2021/10/overcoming-the-growing-risks-to-kids-online/

38 Braue, D. 2021. "Global cybersecurity spending to exceed $1.75 trillion from 2021-2025". Cybercrime Magazine. 10 September 2021. https://cybersecurityventures.com/cybersecurity-spending-2021-2025/; Meeuwisse, R. 2019. "Is effective cybersecurity expensive?" Infosecurity Magazine. 10 April 2019. https://www.infosecurity-magazine.com/blogs/effective-cybersecurity-expensive

39 Marsh. 2021. Global Insurance Market Index Q3 2021. October 2021. https://www.marsh.com/fr/en/services/insurance-market-and-placement/insights/global_insurance_market_index.html

40 Sabbagh, D. 2021. "Experts say China's low-level cyberwar is becoming severe threat". The Guardian. 23 September 2021. https://www.theguardian.com/world/2021/sep/23/experts-china-low-level-cyber-war-severe-threat

41 BBC. 2021. "Aukus: UK, US and Australia launch pact to counter China". BBC. 16 September 2021. https://www.bbc.com/news/world-58564837; Kanno-Youngs, Z. and Sanger, D.E. 2021 "U.S. accuses China of hacking Microsoft". The New York Times. 26 August 2021. https://www.nytimes.com/2021/07/19/us/politics/microsoft-hacking-china-biden.html?; McWhorter, D. 2021. "Exposing one of China's cyber espionage units". Mandiant. https://www.mandiant.com/resources/apt1-exposing-one-of-chinas-cyber-espionage-units

42 Kemp, S. 2021. "Digital 2021 April Global Statshot Report". Datareportal. 26 April 2021. https://datareportal.com/reports/digital-2021-april-global-statshot

43 Rodriguez, K. and Opsahl, K. 2020. "Augmented reality must have augmented privacy". Electronic Frontier Foundation. 16 October 2020. https://www.eff.org/deeplinks/2020/10/augmented-reality-must-have-augmented-privacy

44 Sultan, A. 2021. "Improving Cybersecurity Awareness in Underserved Populations". UC Berkeley Center for Long-Term Cybersecurity White Paper Series. 2021. https://cltc.berkeley.edu/underserved_populations/

45 Kite-Powell, J. 2021. "The rise of voice cloning and deepfakes in the disinformation wars". Forbes. 21 September 2021. https://www.forbes.com/sites/jenniferhicks/2021/09/21/the-rise-of-voice-cloning-and-deep-fakes-in-the-disinformation-wars/?sh=405859e138e1; Nicolls, D. 2019. "Will deepfake technology defeat biometric authentication?" Jumio.com. 10 October 2019. https://www.jumio.com/deepfake-technology-biometric-authentication/; Pipikaite, A. 2021. "How to improve security of biometric data". World Economic Forum Global Agenda. 2 September 2021. https://www.weforum.org/agenda/2021/09/untangling-the-benefits-and-risks-of-biometrics/

46 ISACA. 2021. "State of Cybersecurity 2021: Threat Landscape, Security Operations and Cybersecurity Maturity (Part 2)". ISACA. 2021. https://www.isaca.org/go/state-of-cybersecurity-2021; Kite-Powell, J. 2020. "Here's how 2020 created a tipping point in trust and digital privacy". Forbes. 27 October 2020. https://www.forbes.com/sites/jenniferhicks/2020/10/27/heres-how-2020-created-a-tipping-point-in-trust-and-digital-privacy/?sh=7fe5bc4a4fc5; Lucas, O. 2021. "Corporate data responsibility: Bridging the consumer trust gap". PwC. August 2021. https://advisory.kpmg.us/articles/2021/bridging-the-trust-chasm.html?utm_source=vanity&utm_medium=referral&mid=m-00005652&utm_campaign=c-00107353&cid=c-00107353; Muggah, R. 2021. "Digital privacy comes at a price. Here's how to protect it". World Economic Forum Global Agenda. 8 September 2021. https://www.weforum.org/agenda/2021/09/how-to-protect-

digital-privacy/; NortonLifeLock, Inc. 2021. "Norton Cyber Safety Insights Report: Global Results". Norton and The Harris Poll. May 2021. https://now.symassets.com/content/dam/norton/campaign/NortonReport/2021/2021_NortonLifeLock_Cyber_Safety_Insights_Report_Global_Results.pdf

47 Statista. Most popular global mobile messenger apps as of October 2021, based on number of monthly active users, accessed 14 December 2021. https://www.statista.com/statistics/258749/most-popular-global-mobile-messenger-apps/

48 Privacy International. 2019. "Most cookie banners are deceptive and annoying. This is not privacy". Privacy International. 21 May 2019. https://privacyinternational.org/explainer/2975/most-cookie-banners-are-annoying-and-deceptive-not-consent

49 Kwet, M. 2021. "Digital colonialism: The evolution of US empire". TNI's Future Lab series on Technology, Power and Emancipation organized in collaboration with ROAR magazine. 4 March 2021. https://longreads.tni.org/digital-colonialism-the-evolution-of-us-empire; Ryan-Mosley, T. 2021. "Why you should be more concerned about Internet shutdowns". MIT Technology Review. 9 September 2021. https://www.technologyreview.com/2021/09/09/1035237/internet-shutdowns-censorship-exponential-jigsaw-google/

50 Buckley, J. and Conner, S. 2021. "Cyber threats: Living with disruption". Control Risks and AirMic. 12 October 2021. https://www.controlrisks.com/our-thinking/insights/reports/cyber-threats-living-with-disruption; 2021. "Insurance giant AXA victim of ransomware attack". Security. 19 May 2021. https://www.securitymagazine.com/articles/95245-insurance-giant-axa-victim-of-ransomware-attack

51 Rappeport, A., Kramer, A.E. and Sanger, D.E. 2021. "The Biden administration is combating ransomware with a crackdown on cryptocurrency payments". The New York Times. 21 September 2021. https://www.nytimes.com/2021/09/21/us/politics/treasury-department-combating-ransomware-cryptocurrency.html; U.S. Securities and Exchange Commission. 2021. "SEC Announces Three Actions Charging Deficient Cybersecurity Procedures". Press Release. 30 August 2021. https://www.sec.gov/news/press-release/2021-169

52 Mee, P. and Brandenburg, R. 2020. "After reading, writing and arithmetic, the 4th 'r' of literacy is cyber-risk". World Economic Forum Global Agenda. 17 December 2020. https://www.weforum.org/agenda/2020/12/cyber-risk-cyber-security-education

53 Check Point Software Technologies Ltd. 2021. The Biggest Cloud Security Challenges of 2021. https://www.checkpoint.com/cyber-hub/cloud-security/what-is-cloud-native-security/the-biggest-cloud-security-challenges-in-2021/

CHAPTER 4

Barriers to Migration

200 million

projected climate refugees by 2050

~25%

remittances-to-GDP in El Salvador and Honduras

9%

decline in FDI to low-income countries in 2021

4,800

estimated migrants perished or missing in 2021

REUTERS/YARA NARDI

Nowhere to go

Large parts of the global population face an increasingly insecure outlook (see Chapter 1). Global Risks Perception Survey (GRPS) respondents perceive "livelihood crises" as one of the most potentially severe risks over the next decade. Millions of people are already seeking to cross borders in search of better economic opportunities.

Over the last decade, the number of international migrants has grown consistently, from 221 million people in 2010 to 281 million in 2020.[1] Economic hardship, climate change, conflict and political instability are forcing millions more people to leave their homes. These trends are reflected in the GRPS, where "involuntary migration" is ranked as a top long-term concern.

Better international collaboration is required to manage these flows to ensure that economic migrants are not exposed to exploitation and that involuntary migrants—refugees—crossing into other countries receive the assistance and shelter that they need. The scale of the challenge has put significant pressure on existing frameworks for migration and refugee protection, such as the 1951 Refugee Convention and 1967 Protocol;[2] this pressure is compounded by fractures within the international community and national interest postures that risk limiting global capacity to address this challenge. Some 60% of GRPS respondents believe "migration and refugees" is an area where international mitigation efforts are falling short (that is, they have either "not started" or are in "early development").

Economic migration often has considerable benefits for both origin and destination countries. It is "the most effective way to reduce poverty and share prosperity", according to a World Bank report,[3] and can support economic growth by helping address labour shortages in destination countries. While most cross-border migration takes place between low- and middle-income countries, 83% of non-migrant residents in the 22 richest Organisation for Economic Co-operation and Development (OECD) countries have experienced net economic gains from the influx of migrants.[4] On the other hand, some project-based migration undertakings to enhance cross-border infrastructure have had negative impacts in destination countries, where the

REUTERS/SAEED ALI ACHAKZAI

tendency to employ workers from origin countries has reduced opportunities for income and skills transfer for native, destination-country workers.[5]

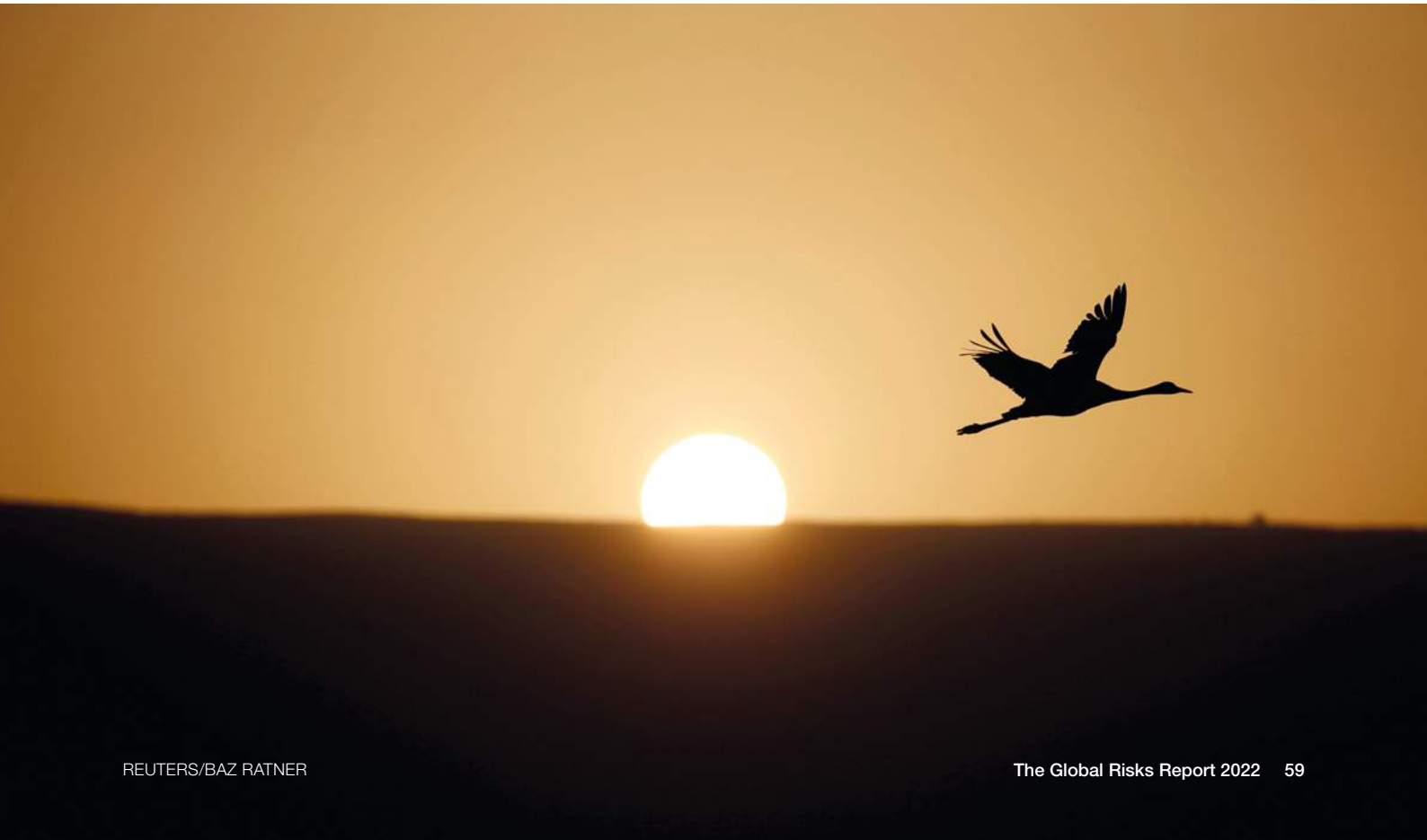
Refugees can also ultimately make a positive contribution to the economies of destination countries, depending partly on a balanced intake across countries that have the capacity to take them in. Their ability to contribute often depends on whether they receive support to deal with the aftereffects of forced displacement—for example, counselling for post-traumatic stress, which is not normally afforded to economic migrants. Instead, millions of refugees remain crowded in camps on the fringes of society—often in countries in the Global South that do not have the economic capacity to absorb them.

However, national-level barriers to the movement of people are increasing. Disillusionment with globalization has fuelled nativist discourses and national interest policies in many destination countries in recent years, and COVID-19 has accelerated this trend. An IPSOS–World Economic Forum Survey from April 2021 found that positive views towards globalization fell during the pandemic by an average of 10 percentage points across 25 countries.[6] Many governments, reflecting popular attitudes, have expressed concern about pressures on education and healthcare services, housing capacity and local employment; for others, integration concerns have been a priority.

Higher barriers to both orderly and disorderly migration elevate the risk of forgoing potential pathways to restoring livelihoods, closing income and labour gaps and maintaining political stability. Instead, the clash between heightened insecurity in origin countries and migration barriers in destination countries will exacerbate global divergence (see Chapter 1), aggravating tensions within and between countries that could complicate an equitable recovery and lead to ever more desperate measures by those who feel compelled to move.

Growing insecurity in origin countries

Movement restrictions related to COVID-19 interrupted some migration flows;[7] as these restrictions are lifted, divergent economic recoveries will likely amplify pressures to migrate that have been restrained through the pandemic.[8] Many origin countries—mostly less advanced and less vaccinated



REUTERS/BAZ RATNER

ones (see Chapter 1)—face highly insecure economic outlooks as growth stagnates, public finances continue to be stretched and pandemic-related stimuli—on which vulnerable groups have depended—are scaled back.[9] Employment in these countries may also decline if the pandemic persists, exacerbated by a worldwide trend for workplace automation, re-shoring business operations and shortening supply chains that may affect foreign direct investment (FDI) inflows, exports and growth.[10] In many lower-income countries, where informal work is prevalent, informal migrant workers are particularly exposed to the pandemic's economic fallout because of their low income and lack of access to state support.[11]

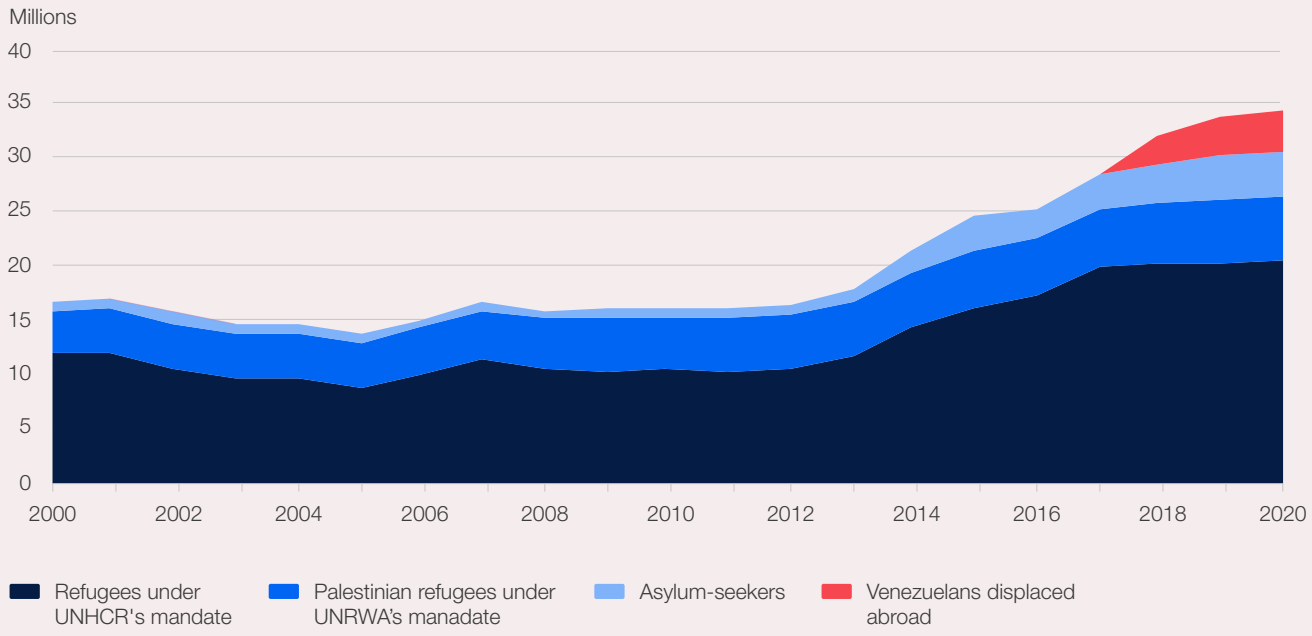
Climate change is a key driver of migration. It displaces people directly because of natural disasters and it can displace them indirectly by encouraging economic migration from weakening economies vulnerable to the adverse impacts of climate change. The inability to adapt to or mitigate the impacts of climate change threaten to make certain densely populated parts of the world uninhabitable.[12] More frequent and extreme weather events—including fires, floods and droughts—could displace more than 200 million people by 2050.[13] Water scarcity is a key driver of migration because of its impact on health and livelihoods as well as the conflicts it risks triggering.[14] GRPS respondents rated "extreme weather" and "climate action failure" as strong aggravators of "involuntary migration". Densely populated countries that are highly dependent on agriculture—such as India, Nigeria, Pakistan and the Philippines[15]—are especially vulnerable to climate insecurity. Worsening extreme weather will trigger large-scale migration and displacement, but the

Climate change, conflict and political instability will force millions to leave their homes

GETTY/MARC GUITARD

FIGURE 4.1

Refugees, Asylum-Seekers and Venezuelans Displaced Abroad, 2000–2020 (Millions)



Source: Data from UNHCR, "Refugee Data Finder". https://www.unhcr.org/refugee-statistics/download/?url=rVpdj6, accessed 1 December 2021.

Note: UNHCR = United Nations High Commissioner for Refugees; UNRWA = United Nations Relief and Works Agency.

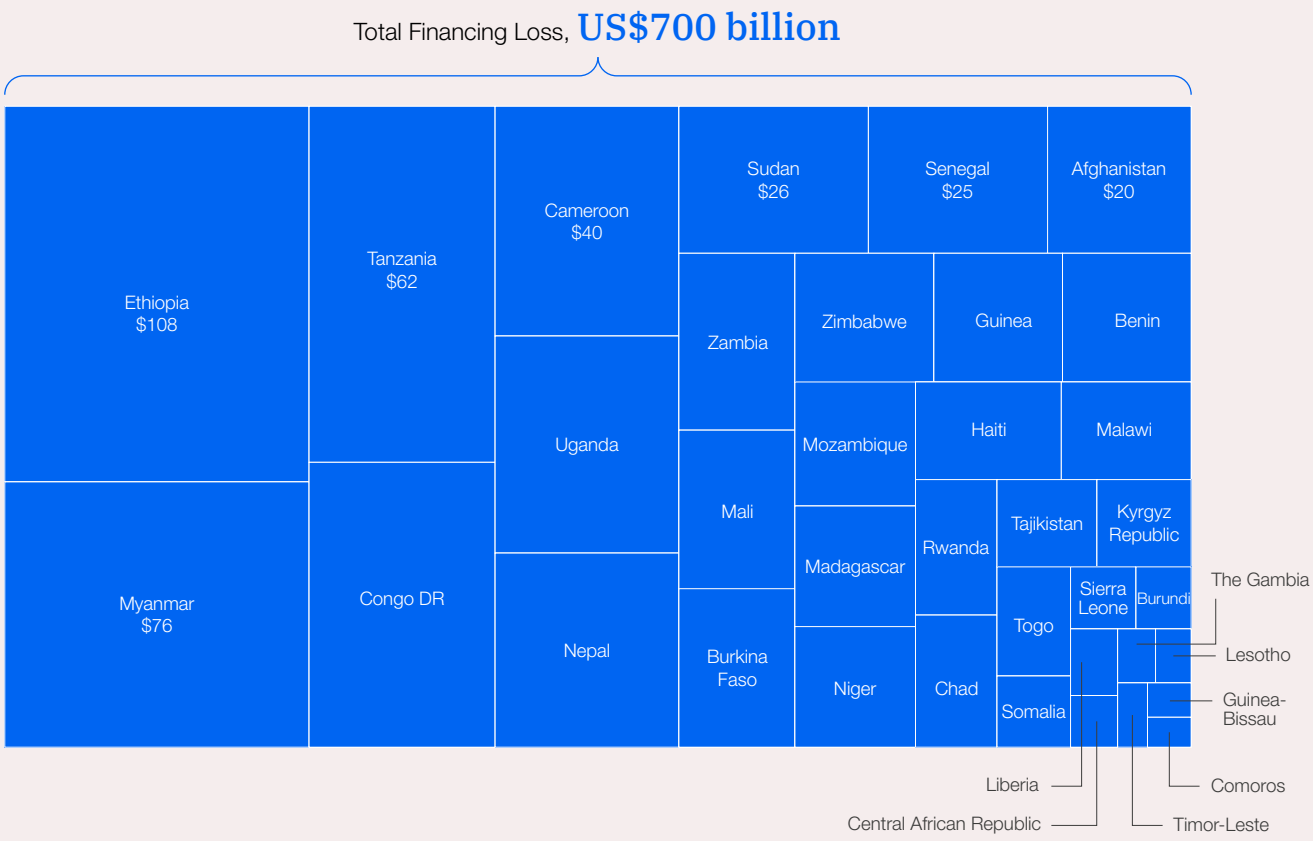
international community's reluctance to recognize "climate refugees" and "environmental migrants" is widening their legal protection gap.[16] Legislative and governance frameworks remain ill-equipped to protect millions at risk of displacement who do not qualify as traditional refugees.[17] These governance voids could leave governments blindsided in the event of a sudden, high-impact environmental shock. Moreover, the failure to achieve inclusive transitions to net zero economies (see Chapter 2) could worsen economic insecurity for businesses and households in those origin countries left behind.

Conflict and political insecurity are also major drivers of involuntary migration. In 2020, there were over 34 million people displaced abroad globally from conflict alone—a historical high (see Figure 4.1)—mostly due to long-standing conflicts and political turmoil in Afghanistan, Myanmar, South Sudan, Syria and Venezuela,[18] and to expanding conflicts within and beyond the borders of Ethiopia.[19] According to the Executive Opinion Survey (EOS), "involuntary migration" is a top short-term threat in Armenia, Ukraine and Venezuela, which have experienced conflict and political instability.[20] Political turmoil may well worsen in the aftermath of the COVID-19 pandemic, compounded by the reduction of international security forces from conflict zones such as Afghanistan and the Sahel region of Africa. Moreover, some political leaders have reacted to economic crises and social unrest with authoritarianism, discriminatory policies, or extremist discourses that put ethnic or religious minorities at risk of marginalization or violence.

National-level barriers to the movement of people are increasing

FIGURE 4.2

Developing Countries' Financing Loss versus GDP, 2020 (US$ billions)



Source: Data from OECD. Global Outlook on Financing for Sustainable Development 2021. https://www.oecd.org/development/global-outlook-on-financing-for-sustainable-development-2021-e3c30a9a-en.htm; World Bank Open Data, "GDP (current US$)" and "GDP per capita (current US$)". https://data.worldbank.org/indicator/NY.GDP.MKTP.CD, accessed 1 December 2021.

Global cooperation to resolve or mitigate ongoing humanitarian crises is being challenged by financial pressures in advanced economies, greater focus on domestic priorities and a more tense geopolitical context (see Chapter 1). Already, the pandemic has diminished external financing to developing countries by US$700 billion—equivalent to the combined GDPs of 36 of the world's poorest economies (see Figure 4.2).[21]

Mobility barriers in destination countries

There are three potential barriers to cross-border migration: post-pandemic effects on international mobility, future employment trends and increased national interest postures of many countries.

The COVID-19 pandemic and its economic ramifications have emboldened some groups and political leaders to adopt more hostile postures against migration, foreigners or communities with foreign roots. Restrictions on international movement as a result of the pandemic remained in place in 32 countries at the time of writing.[22] These include critical destination and corridor countries such as China, India, Russia, the United Arab Emirates and the United States. Future easing of restrictions will depend on the progress of vaccination and the evolution of COVID-19, but persistent vaccination gaps globally, and particularly within origin countries, means international mobility will continue to be restricted for many.

The pandemic may also narrow future employment opportunities for migrant workers in destination countries, both

because of the economic disruption it created and because of the accelerating automation and digitalization of tasks and services. The World Economic Forum's *Future of Jobs Report* found that 50% of employers globally planned to automate tasks in response to COVID-19, often in sectors that have relied on migrant workers.[23] The report also estimates that 85 million jobs will be destroyed by automation by 2025, and although 97 million new jobs will emerge, these jobs may not necessarily match the skillsets of many migrants.[24] The short-term economic rebound from the pandemic has resulted in a surge in hiring in some key sectors for migrants such as hospitality and healthcare, but in the long-term, new consumption patterns in destination countries—such as more e-commerce and less business travel—are expected to shrink demand for jobs in migrant-intensive industries such as agriculture, food services and warehousing.[25]

National interest postures have also become more entrenched across both developing and advanced economies. For example, Chile and Peru have reframed their migration governance mechanisms, which complicates access for migrant and refugee populations to essential financial and healthcare services.[26] Meanwhile, restrictive policies originally grounded in public health concerns have not been rolled back, as indicated by sustained declines in issued visas for the United Kingdom and the perpetuation of Title 42 expulsions at the US border.[27] Other destination countries have sought to harden borders to prevent the arrival of involuntary migrants, as evidenced in fresh ambitions to build walls in Europe and Turkey.[28]

Consequences

Barriers to orderly migration could have negative global consequences, such as widening labour gaps and income disparity, triggering or worsening humanitarian crises and increasing societal polarization.

Economic consequences. The economic rebound from COVID-19 has created labour shortages in specific industries—albeit some may be temporary—by disrupting market dynamics and supply chains and prompting workers to re-evaluate their personal and career choices. At the time of writing, the United States faced over 11 million unfilled jobs in general and the European Union had a deficit of 400,000 drivers just in the trucking industry.[29] The hospitality sector, one of the most severely affected by the pandemic, is especially vulnerable to long-term labour shortages that migration could close. In the United States, a survey found that over 50% of former hospitality employees would not return to their previous jobs, and 60% of workers seeking employment would not consider the hospitality sector.[30]

A decrease in migrant employment could weaken the global flow of remittances such that growth in income fails to keep pace with inflation, thereby limiting social mobility in origin countries. Remittances also support private consumption, savings and investment in origin countries and can equate to a significant proportion of GDP (from nearly one-fourth of GDP in El Salvador and Honduras to over one-third in Somalia).[31] They proved to be resilient through the pandemic, falling by 2% annually in low- and middle-income countries in 2020[32]—far less than the 30% drop in FDI[33]—and quickly recovering to rise by 7.3% in 2021.[34] Combined with stagnant tourism and pressures on exports,[35] a fall in remittances would weaken another important source of financing for many developing countries.

Businesses risk worker deficits and demand shocks from constrained migration

GETTY/PAUL RATJE

Humanitarian consequences. Humanitarian crises could worsen where barriers to exit prevent vulnerable groups from escaping persecution or violence. In some fragile states, governments could block their citizens' departure to halt depopulation as well as capital flight. In Afghanistan and Myanmar, governments have reportedly impeded citizens from leaving the country.[36] Blocking emigration prevents people from seeking more secure livelihoods and diasporas from reuniting with families. It can exacerbate societal fractures by closing a mechanism to reduce poverty and narrow inequality, fuelling citizens' animosity towards government and potentially empowering criminal or even terrorist groups that offer hope to disaffected individuals.

More limited international mobility opportunities will push migrants to embark on more perilous journeys and risk worsening or triggering humanitarian crises in neighbouring and corridor countries. One such case is the Syrian crisis, which by 2021 had already displaced nearly 6 million Syrians abroad—mostly to Turkey, Lebanon and Jordan—but could further deteriorate.[37] An estimated 700,000 Central American migrants transited through Mexico in 2021—a rapid return to pre-pandemic levels[38]—and those unable to enter the United States are unlikely to return to their origin countries.[39] At one point, 15,000 Central American refugees were stranded for days in precarious conditions under a bridge on the Mexico-US border.[40] According to the EOS, "involuntary migration" is a top short-term threat in El Salvador, Guatemala, Honduras and Nicaragua.

These perilous journeys can also lead to tragic loss of life, such as when people become lost at sea or face harsh weather while stuck in borderlands.[41] At the time of writing, nearly 4,800 migrants were estimated to have perished or gone missing in 2021, most of them trying to reach Europe from Africa.[42] Although there is worldwide consensus on the urgent need to combat human trafficking, the International Organization for Migration estimates that organized human-trafficking groups operate in every country.[43]

Geopolitical consequences. Migration pressures could exacerbate geopolitical tensions and even fuel cross-border conflicts. For example, in the Middle East, half a million Afghans are expected

to take increasingly drastic measures to circumvent migration restrictions and flee to neighbouring countries[44]—including Iran, which has enlarged its military presence along the border to deter a potential Taliban incursion.[45] Management of migration flows has become a tense issue between Turkey, which hosts some 3.6 million Syrian refugees,[46] and the European Union.

Geopolitical rifts could also worsen—and new ones emerge—if origin country migration is increasingly used as a geopolitical instrument. The crossing of migrants from Morocco into the Spanish enclave of Ceuta aggravated tensions that originated in the European Union's lack of support for Morocco's claims over the Western Sahara.[47] Political tensions between Belarus and the European Union escalated considerably as Belarus encouraged travel from the Middle East, moved migrants to camps along its border with Poland and pushed them to cross over, prompting Poland to deploy troops in response.[48] In such cases, destination-country governments seeking to comply with international laws on the treatment of refugees—thereby preserving their reputation among the global community in the spheres of global development and human rights—will have to carefully manage diplomatic relationships with neighbours to arrive at a way forward while responding to immigrant scepticism among a significant proportion of their populations.

Geopolitical rifts could worsen if migration is used as a geopolitical instrument

Consequences for stakeholders

People, governments and businesses in origin and destination countries face distinct challenges from divergent perspectives on migration. But stakeholders in both geographies also face common challenges: social unrest if migration is used to discriminate against and marginalize certain groups; hardening political contexts if governments exploit migration challenges to justify more control over citizens and markets; and some negative economic

GETTY

consequences if legitimate diaspora networks in destination countries created by migration are undermined.

Left alone: Consequences for people
By 2020, there were more than 4 million stateless persons in the world, the highest number in a decade;[49] but this number risks increasing due to heightened social polarization and strained government capacity. Limited options for migrants to gain admittance to destination countries upon entry—even temporarily—could be compounded by corridor countries refusing to allow them to remain within their borders. People in this situation—who are unwilling or unable to return home and whose governments do not take responsibility for their welfare—are at risk of being stranded in irregular settlements or facilities with minimal access to basic goods and services, financial support or diplomatic assistance. Others unable to escape insecurity are at risk of violence or falling prey to extremist ideologies and organizations. Refugees would face poor conditions and even violence in transit and in camps if international cooperation to manage involuntary migration is lacking. Even more economic migrants could resort to desperate measures and become vulnerable to exploitation by human-smuggling cartels.

In destination countries, growing extremism could create greater challenges for migrants trying to assimilate.[50] Citizens could also see their civil liberties violated by governments using migration management to justify widespread population surveillance and intrusions on personal information.

Last resort: Consequences for governments
Remittances improve living standards in origin countries and provide an important source of financing.[51] Without them, governments in origin countries whose economic stability hinges on remittances may face severe complications in their ability to govern—some could be at risk of degenerating into failed states. Destination-country governments also face risks domestically from failing to address citizens' concerns with migration. Adopting stricter migration measures could encounter some popular backlash as pro-migration advocates make their voices heard on the streets and online, while failing to effectively manage inflows risks stoking the growth of populism.

Shocks to Reflect Upon

Not in My Country

What if xenophobic political parties in federal democracies start winning more elections and securing leadership positions in destination-country border or sanctuary towns? What if they ignore federal law and start taking border protection or mobility policies into their own hands, facilitating vigilante behaviour?

Show Me the Money

What if stricter migration policies lead to more burdensome regulation, reduced competition and higher fees in remittance services? What if traditional remittance channels are choked off and cryptocurrencies become the prevalent method for sending remittances, exposing digitally insecure migrants to cybertheft?

Too Little, Too Late

What if stalled or delayed climate action means that ecosystems reach their tipping points suddenly and unexpectedly, accelerating climate migration into neighbouring countries as droughts, floods and resource scarcity worsen?

GETTY/JIM WATSON

Little room: Consequences for businesses

Businesses in destination countries are at risk from a global worker deficit and demand-side shocks that could result from constrained migration. Migrant workers comprise an attractive consumer group that can contribute to developing domestic markets and support international expansion by boosting brand awareness in their home countries. But businesses perceived to favour stricter foreign labour requirements, or that are seen as not making enough effort to support their migrant staff, could face a public backlash from migrant communities and their supporters. On the other hand, businesses that welcome migrant workers with a view to low-cost labour may expose themselves to union pushback.

Towards two-way bridges

At a time of global divergence, migration could foster economic integration. International mobility could narrow inequality within and between countries by matching job seekers in origin countries with unfulfilled vacancies abroad in growth industries—such as healthcare, renewable energy and transportation.[52]

More efficient and orderly channels for migration—including coherent legal and policy frameworks, cross-border cooperation and alignment and better enforcement against smuggling operations—could prompt closer political ties between countries and encourage collaboration on issues of mutual concern such as shared infrastructure for cross-border financial flows. The global community could also build goodwill across geopolitical divisions by strengthening collaboration mechanisms for refugee intake.

Migration offers opportunities but also entails challenges for origin, corridor and destination countries. Leaders have the chance to jointly identify where new bridges can be built for mutual benefit.

Endnotes

1 United Nations Population Division, "International Migrant Stock". https://www.un.org/development/desa/pd/content/international-migrant-stock, accessed 17 December 2021

2 UNHCR (United Nations High Commissioner for Refugees). 1951. "The 1951 Convention Relating to the Status of Refugees and its 1967 Protocol". UNHCR. 25 July 1951. https://www.unhcr.org/about-us/background/4ec262df9/1951-convention-relating-status-refugees-its-1967-protocol.html

3 World Bank. 2018. Moving for Prosperity: Global Migration and Labor Markets. Policy Research Report. World Bank Group. 15 June 2018. https://www.worldbank.org/en/research/publication/moving-for-prosperity

4 Aubry, A., Burzyński, M. and Docquier, F. 2016. "The welfare impact of global migration in OECD countries". Journal of International Economics, Volume 101. July 2016. https://www.sciencedirect.com/science/article/abs/pii/S002219961630040X

5 Hillman, J. and Tippett, A. 2021. "Who built that? Labor and the Belt and Road Initiative". Council on Foreign Relations. 6 July 2021. https://www.cfr.org/blog/who-built-labor-and-belt-and-road-initiative

6 IPSOS. 2021. "World Opinion on Globalization and International Trade in 2021". Ipsos Global Advisor 25-Country Survey for the World Economic Forum. IPSOS. August 2021. https://www.ipsos.com/en/sentiment-about-globalization-cooler-pandemic-across-world

7 International Organization for Migration. 2021. Global Mobility Restriction Overview. Weekly Update. IOM. 4 October 2021. https://migration.iom.int/reports/covid-19-travel-restrictions-output-%E2%80%94-4-october-2021?close=true

8 International Centre for Migration Policy Development. 2021. "ICMPD migration outlook 2021. Seven things to look out for in 2021". ICMPD. 26 January 2021. https://www.icmpd.org/file/download/50542/file/ICMPD_Migration_Outlook_2021_final.pdf

9 IMF (International Monetary Fund). "Policy Responses to COVID-19". Policy Tracker. https://www.imf.org/en/Topics/imf-and-covid19/Policy-Responses-to-COVID-19#B, accessed 3 December 2021.

10 Mercer. 2021. "Win with empathy. Global Talent Trends 2020-2021". 8 February 2021. https://www.mercer.com/our-thinking/career/global-talent-hr-trends.html; Milne, R. and Dempsey, H. 2021. "Suez blockage will accelerate global supply chain shift, says Maersk chief". Financial Times. 29 March 2021. https://www.ft.com/content/e9452046-e88e-459a-9c54-341c85f3cb0d; Reinsch, W.A., Benson, E., Lim, J., Hokayem, A. and Mortensen, S. 2021. The Manufacturer's Dilemma: Reshoring and Resiliency in a Pandemic World. Center for Strategic and International Studies. https://www.csis.org/analysis/manufacturers-dilemma-reshoring-and-resiliency-pandemic-world; World Economic Forum. 2020. The Future of Jobs Report 2020. October 2020. https://www3.weforum.org/docs/WEF_Future_of_Jobs_2020.pdf

11 Fleming, S. 2020. "This is how COVID-19 is affecting informal workers". World Economic Forum. 29 July 2020. https://www.weforum.org/agenda/2020/07/coronavirus-impact-informal-workers-world-bank/

12 World Economic Forum, in partnership with Marsh & McLennan Companies and Zurich Insurance Group. 2020. The Global Risks Report 2020. Insight Report. Chapter 3 A Decade Left. Geneva: World Economic Forum. January 2020. https://www.weforum.org/reports/the-global-risks-report-2020

13 World Bank. 2021. Groundswell Part 2: Acting on Internal Climate Migration. Report. Open Knowledge Repository. World Bank Group. September 2021. https://openknowledge.worldbank.org/handle/10986/36248

14 UNHCR. 2021. Global Report 2020. UNHCR. 2020. https://www.unhcr.org/flagship-reports/globalreport/; Rachman, G. 2021. "The threat of conflict over water is growing". Financial Times. 1 November 2021. https://www.ft.com/content/ b29578f1-c05f-4374-bbb4-68485ef6dbf7

15 World Bank Open Data. "Agriculture, forestry, and fishing, value added (% of GDP)". https://data.worldbank.org/indicator/NV.AGR.TOTL.ZS, accessed 2 December 2021.

16 Rameez Raza, M. and Shekhar, R. 2020. "Climate Crisis, Migration and Refugees: Bridging the Legal Protection Gap for a Sustainable Future". RLI Blog on Refugee Law and Forced Migration. School of Advanced Study, University of London. 29 July 2020. https://rli.blogs.sas.ac.uk/2020/07/29/climate-crisis-migration-and-refugees-bridging-the-legal-protection-gap-for-a-sustainable-future/

17 Apap, J. and Perron de Revel, C. 2021. "The concept of 'climate refugee'. Towards a possible definition." Briefing. European Parliamentary Research Service. October 2021. https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698753/EPRS_BRI(2021)698753_EN.pdf

18 UNHCR. 2021. Global Trends in Forced Displacement – 2020. UNHCR. 18 June 2021. https://www.unhcr.org/60b638e37/unhcr-global-trends-2020

19 UNHCR. 2021. "Eritrean refugees in Tigray caught up in conflict". Press Briefing. 27 July 2021. https://www.unhcr.org/news/briefing/2021/7/60ffc4d44/eritrean-refugees-tigray-caught-conflict.html

20 Council on Foreign Relations. 2021. "Nagorno-Karabakh Conflict" and "Conflict in Ukraine". Global Conflict Tracker. https://www.cfr.org/global-conflict-tracker/?category=us, accessed 3 December 2021.

21 OECD (Organisation for Economic Cooperation and Development). 2021. Global Outlook on Financing for Sustainable Development 2021: A New Way to Invest for People and Planet. OECD. https://www.oecd-ilibrary.org/sites/e3c30a9a-en/1/3/1/index.html?itemId=/content/publication/e3c30a9a-en&_csp_=8cdd8991f371dde0be547aab4112527a&itemIGO=oecd&itemContentType=book; World Bank Open Data. "GDP (current US$)" and "GDP per capita (current US$)". https://data.worldbank.org/indicator/NY.GDP.MKTP.CD and https://data.worldbank.org/indicator/NY.GDP.PCAP.CD?most_recent_value_desc=false, accessed 1 December 2021.

22 Blavatnik School of Government. "Covid-19 Government Response Tracker". University of Oxford. https://www.bsg.ox.ac.uk/research/research-projects/covid-19-government-response-tracker, accessed 7 December 2021.

23 World Economic Forum. 2020. The Future of Jobs Report 2020. October 2020. https://www3.weforum.org/docs/WEF_Future_of_Jobs_2020.pdf

24 Ibid.

25 McKinsey Global Institute. 2021. The Future of Work after COVID-19. Report. McKinsey & Company. 18 February 2021. https://www.mckinsey.com/featured-insights/future-of-work/the-future-of-work-after-covid-19

26 Freier, L.F. and Vera Espinoza, M., 2021. "COVID-19 and immigrants' increased exclusion: The politics of immigrant integration in Chile and Peru". Frontiers in Human Dynamics 3: 6. https://www.frontiersin.org/articles/10.3389/fhumd.2021.606871/full

27 Constantino, A. K. 2021. "U.S. defends expulsion of undocumented migrants under health policy, even as it eases border restrictions for travelers with visas". CNBC. 13 October 2021. https://www.cnbc.com/2021/10/13/us-defends-expelling-migrants-as-canada-mexico-border-restrictions-ease.html; GOV.UK. "Summary of latest statistics. Immigration statistics, year ending June 2021". Cabinet Office Government Digital Service. https://www.gov.uk/government/statistics/immigration-statistics-year-ending-june-2021/summary-of-latest-statistics, accessed 21 December 2021; Somerville, W. and Walsh, P.W. 2021. "United Kingdom's decades-long immigration shift interrupted by Brexit and the pandemic". Migration Policy Institute. 19 August 2021. https://www.migrationpolicy.org/article/united-kingdom-shift-immigration-interrupted-brexit-pandemic; US Customs and Border Protection. "Nationwide Enforcement Encounters: Title 8 Enforcement Actions and Title 42 Expulsions 2022". CBP Enforcement Statistics. https://www.cbp.gov/newsroom/stats/cbp-enforcement-statistics/title-8-and-title-42-statistics, accessed 21 December 2021.

28 Follain, J. 2021. "EU should pay for walls against migrants, 12 nations tell bloc". Bloomberg. 8 October 2021. https://www.bloomberg.com/news/articles/2021-10-08/eu-should-pay-for-walls-against-migrants-12-nations-tell-bloc; Yackley, A. J. 2021. "The Turkish wall built to keep out refugees from Afghanistan". Financial Times. 15 September 2021. https://www.ft.com/content/49d85b11-4bbe-4518-b6d8-d532e30c373c

29 Arnold, M. and Vladkov, A. 2021. "Europe's trucker shortage becoming 'extremely dangerous'". Financial Times. 13 October 2021. https://www.ft.com/content/e8ca2a08-308c-4324-8ed2-d788b074aa6c; US Bureau of Labor Statistics. 2021. "Job Openings and Labor Turnover Summary". Economic News Release. USBLS. 8 December 2021. https://www.bls.gov/news.release/jolts.nr0.htm

30 Joblist. 2021. "Q2 2021 United States job market report". Job Market Reports. Joblist. 8 July 2021. https://www.joblist.com/jobs-reports/q2-2021-united-states-job-market-report

31 World Bank Open Data. "Personal remittances, received (% of GDP)". https://data.worldbank.org/indicator/BX.TRF.PWKR.DT.GD.ZS?most_recent_value_desc=true, accessed 14 December 2021

32 World Bank. 2021. "Defying Predictions, Remittance Flows Remain Strong During COVID-19 Crisis". Press Release. World Bank Group. 12 May 2021. https://www.worldbank.org/en/news/press-release/2021/05/12/defying-predictions-remittance-flows-remain-strong-during-covid-19-crisis

33 Ibid.

34 Dilip, R. 2021. "Global Remittance Flows in 2021: A Year of Recovery and Surprises". World Bank Blogs. World Bank Group. 17 November 2021. https://blogs.worldbank.org/peoplemove/global-remittance-flows-2021-year-recovery-and-surprises

35 United Nations World Tourism Organization. 2021. "Global tourism sees upturn in Q3 but recovery remains fragile". UNWTO. 28 November 2021. https://www.unwto.org/taxonomy/term/347; World Bank Open Data. "Exports of goods and services (% of GDP) - Low & middle income". https://data.worldbank.org/indicator/NE.EXP.GNFS.ZS?locations=XO, accessed 2 December 2021.

36 Gannon, K. 2021. "Taliban stop planes of evacuees from leaving but unclear why". AP News. 5 September 2021. https://apnews.com/article/middle-east-religion-taliban-dbe38a9a3c0b33f3532aac5ff1b50078; Myanmar Now. "Workers trying to leave Myanmar turned away at airports after junta tightens rules". Myanmar Now. 21 October 2021. https://www.myanmar-now.org/en/news/workers-trying-to-leave-myanmar-turned-away-at-airports-after-junta-tightens-rules

37 UNHCR. 2021. Operational Data Portal. Refugee Situations. "Syria Refugee Regional Response". https://data2.unhcr.org/en/situations/syria, accessed 6 January 2022.

38 Congressional Research Service. 2021. "Central American migration: Root causes and U.S. policy". In Focus. 27 October 2021. https://sgp.fas.org/crs/row/IF11151.pdf

39 NPR (National Public Radio). 2021. "How the southern U.S. border has become a nearly constant humanitarian crisis". Interview with Alicia Schmidt Camacho in "All Things Considered". NPR. 24 September 2021. https://www.npr.org/2021/09/24/1040550699/how-the-southern-u-s-border-has-become-a-nearly-constant-humanitarian-crisis

40 Gonzalez, V. and Spagat, E. 2021. "Inside Biden's border plans: How optimism turned to chaos". AP News. 3 November 2021. https://apnews.com/article/immigration-coronavirus-pandemic-donald-trump-joe-biden-health-af698c3434cc31dfbce43a66fbf43b49

41 ECRE (European Council on Refugees and Exiles). 2020. "Bosnia and Herzegovina: Snowfall increases hardships of people stuck in Europe's borderlands". Ecre News. 11 December 2020. https://ecre.org/bosnia-and-herzegovina-snowfall-increases-hardships-of-people-stuck-in-europes-borderlands/; UN News. 2021. "Drowning of 27 migrants in English Channel is worst disaster on record: IOM". United Nations. 25 November 2021. https://news.un.org/en/story/2021/11/1106562

42 Missing Migrants Project. "Dead and Missing by Year". IOM. https://missingmigrants.iom.int/data, accessed 23 December 2021.

43 International Organization for Migration. 2021. World Migration Report 2022. IOM. https://worldmigrationreport.iom.int/wmr-2022-interactive/

44 UNHCR. 2021. "Afghanistan Situation Regional Refugee Preparedness and Response Plan". Operational Data Portal. UNHCR. 27 August 2021. https://data2.unhcr.org/en/documents/details/88385

45 Nadimi, F. 2021. "Iran sets its eyes on Afghanistan". Policy Analysis. The Washington Institute for Near East Policy. 19 July 2021. https://www.washingtoninstitute.org/policy-analysis/iran-sets-its-eyes-afghanistan

46 UNHCR. 2021. "Refugees and Asylum Seekers in Turkey". UNHCR. https://www.unhcr.org/tr/en/refugees-and-asylum-seekers-in-turkey

47 Casey, N. and Bautista, J. 2021. "'Come on in, boys': A wave of the hand sets off Spain-Morocco migrant fight". New York Times. 2 June 2021. https://www.nytimes.com/2021/06/02/world/europe/spain-ceuta-migrants-morocco.html; Torreblanca, J. I. 2021. "This time is different: Spain, Morocco, and weaponised migration". Commentary. European Council on Foreign Relations. 26 May 2021. https://ecfr.eu/article/this-time-is-different-spain-morocco-and-weaponised-migration/

48 Emmott, R. 2020. "EU says Lukashenko is not legitimate Belarus president". Reuters. 24 September 2020. https://www.reuters.com/article/us-belarus-election-eu-idUSKCN26F0ZE; Pempel, K. and Kiselyova, M. 2021. "'Go through. Go,' Lukashenko tells migrants at Polish border". Reuters. 26 November 2021. https://www.reuters.com/world/europe/lukashenko-tells-migrants-belarus-poland-border-he-wont-make-them-go-home-2021-11-26/

49 UNHCR. 2021. "Global Trends in Forced Displacement – 2020". Op. cit.

50 International Organization for Migration. 2019. World Migration Report 2020. IOM. 2019. https://publications.iom.int/system/files/pdf/wmr_2020.pdf

51 World Bank. 2018. Op. cit.

52 McKinsey Global Institute. 2021. Op. cit.

CHAPTER 5

Crowding and Competition in Space

5

number of new government-developed space stations by 2030

70,000

estimated number of satellites to launch in coming decades

28

nations with domestic space regulation

1 million

estimated number of debris pieces 1 centimetre and larger

REUTERS/ROSCOSMOS

Space is getting busier

Humans have been inspired by space exploration for decades but growing commercial and geopolitical interests are increasingly influencing this frontier. While early space activity was conducted or funded by the public sector, the last decade has seen growing private investment. New commercial entrants are disrupting traditional incumbents' control in delivering satellite services, especially in internet-related communications or launch services. Some governments are encouraging private space activity to further national "territorial" claims or to foster the development of high-value jobs, especially in the zone of Low Earth Orbit (LEO) or Medium Earth Orbit (MEO), as well as enhancing their military or defence-oriented presence.* Increased exploitation of these orbits carries the risk of congestion, an increase in debris and the possibility of collisions in a realm with few governance structures to mitigate new threats.

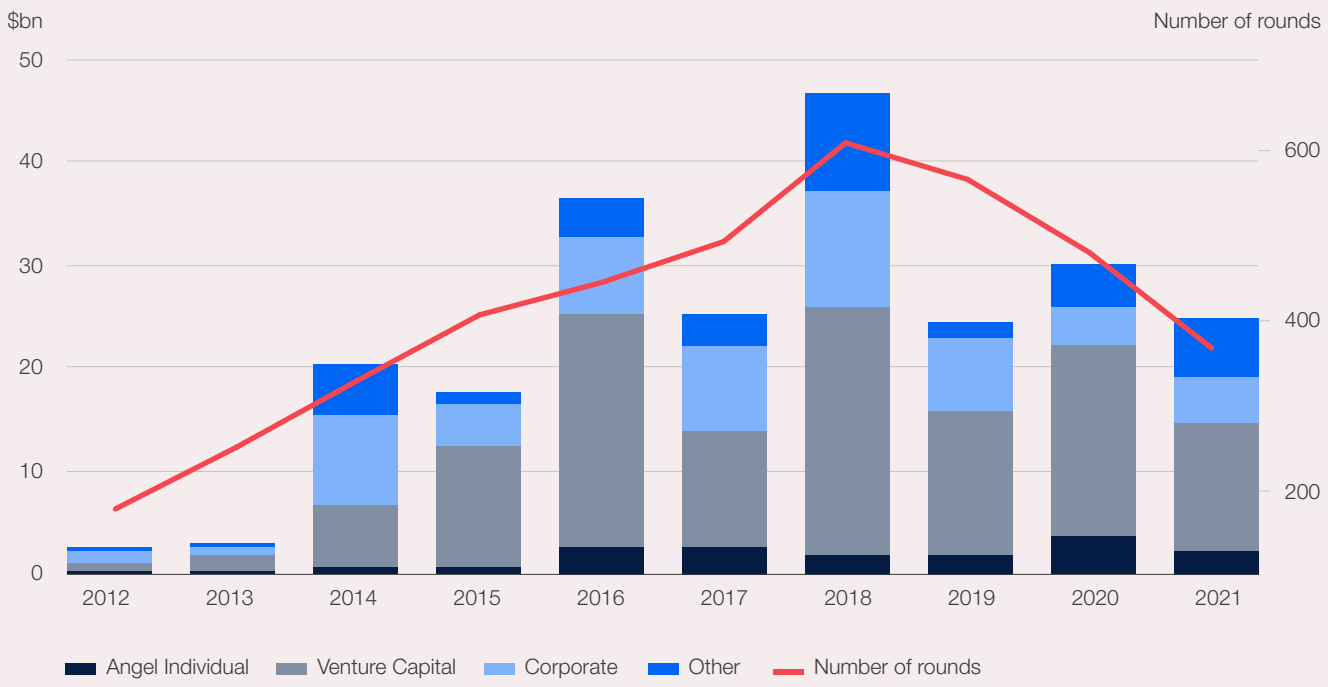
A LEO/MEO space race

The traditional Geostationary Orbit (GEO) commercial satellite market, which has dominated the communications sector for decades, is now losing commercial value because of competition from new players seeking to provide services from LEO or MEO. More recently, in the last decade, the financing of new applications for space-based initiatives has grown fast: businesses, start-ups and research entities are proliferating, raising money in the billions, and thereby driving down the cost of launch systems, particularly in LEO (see Figure 5.1).[1] Lower costs bring more opportunity for a greater diversity of actors to launch constellations of smaller satellites. With this more cost-effective access to space, attention is increasingly shifting to new opportunities in areas such as hyperspectral remote sensing, energy

* Low Earth Orbit (LEO) is generally considered to encompass Earth-centred orbits with an altitude of 2,000 kilometres (1,200 miles) or less. The Geostationary Orbit (GEO) encompasses a higher-altitude orbit, typically at an altitude of 35,000 kilometres above the Earth's equator while Medium Earth Orbit (MEO) comprises a range of orbits between LEO and GEO.

FIGURE 5.1

Space Investment: Equity Capital by Investor Type (US$ Billions)



Source: Space Capital. Q3 2021. https://app.powerbi.com/view?r=eyJrIjoiNGY4MWI4OWEtMjNmZS00OTM3LWE5M2QtYTgxZTdjODk3YTIlIiwidCI6IjYzMDZkMTJjLTEwODMtNGNhOS04Yjk2LTdjYzM3ODcwMWIzMiIsImMiOjN9

generation, manufacturing, mining and tourism.[2] However, the largest growth is still expected to come from industries that are already expanding digital connectivity on Earth, such as direct-to-consumer broadband access.[3]

Businesses, start-ups and research entities are proliferating

National ambitions

Space programmes are still widely seen as a sign of national prestige, as they project geopolitical and military power as well as have scientific and commercial significance. Powers such as China, Europe (EU and ESA), France, Germany, India, Japan, NATO, Russia, the United Kingdom and the United States have publicly announced space forces and continue to build space infrastructure, with plans for at least five new space stations by 2030 in the works.[4] The first commercial space station is also slated for completion in the next decade.[5] Next-step deep space exploration projects are under development, such as the United States–led Artemis programme—which aims to reopen exploration of the Moon and eventually develop outposts on Mars and asteroids.[6] In addition, new space-faring powers will emerge as more economies begin to see opportunities to expand both geopolitical and commercial influence in this arena. Among countries that have expressed interest are Argentina, Brazil, and Mexico in Latin America; Egypt, Iran, Turkey, Saudi Arabia, South Africa and the United Arab Emirates in Africa and the Middle East; and Australia, Indonesia, Malaysia, New Zealand, South Korea and Vietnam in the Asia-Pacific region.[7]

Alongside new programme development, the critical infrastructure on which many civil and commercial entities rely must be maintained and secured.[8] Satellites in LEO as well as in MEO and GEO are used for multiple purposes that include climate and natural resource monitoring, broadband internet, and radio and television broadcasting, as well as position,

REUTERS/ALY SONG

navigation and timing services.[9] While this infrastructure will continue to remain vital for governments, businesses and societies, it is also creating opportunities for nations with an advanced space industry, supported by national-level regulation, to stake claims to specific orbital sectors by virtue of first-mover advantage.[10] Finally, space will continue to be of critical military importance: armed forces have long relied on space-based or space-supported technologies—including Global Positioning System (GPS) for navigation, dedicated military satellite-based communications for secure digital connectivity and spy satellites for intelligence—making such systems tempting military targets and spurring the need for enhanced defensive measures.[11]

Consequences

A greater number and diversity of actors operating in space could generate new or exacerbate old frictions if not responsibly managed. The trend in commercial, civil and military sectors is to replace traditionally large and expensive single geostationary satellite systems with a more distributed system of multiple smaller satellites in LEO. Approximately 11,000 satellites have been launched since Sputnik 1 in 1957, but 70,000 more could enter orbit in the coming decades if proposed plans play out.[12] The vast majority of these new planned and approved satellites will be launched by a handful of operators that will have increasing influence over the regulatory landscape.

Once in orbit, and unless actively decommissioned, many of these satellites could remain in space for hundreds of years.[13] Smaller, low-cost satellites are also proliferating because of lower costs and fewer barriers to entry.[14] While the risk is still relatively low, an increase in the number of satellites also increases the opportunity for collisions, or, at the least, a need to engage in emergency manoeuvres to avoid contact.

Collisions could hinder future space development or aggravate international tensions. This is because when objects in space collide, they may break up and produce debris that—even at sizes of 1 to 5 centimetres in diameter—could cause severe damage.[15] For example, the International Space Station (ISS) was damaged in May 2021 when a piece of debris penetrated its robotic arm.[16] Such strikes have been documented for decades, but they may become more frequent. One theory, known as the "Kessler Effect" (see Box 5.1), posits the potential consequences of a cascading effect.[17] Estimates put the current number of smaller pieces of debris (larger than 1 centimetre in size) at nearly a million,[18] while larger objects over 10 centimetres number in the thousands (see Figure 5.2). Providing orbital servicing and debris removal could, however, help alleviate some of the worst consequences.[19] Tracking debris is a critical tool in preventing collision or damage, but it will need to become increasingly sophisticated to maintain reliability in a more congested realm.

With such possibilities becoming likelier in a congested space, the lack of updated international rules around space activity increases the risk of potential clashes. The most relevant of space agreements, the Outer Space Treaty, was concluded in 1967 and still, through the UN Office for

BOX 5.1

The Kessler Effect

First identified by NASA scientist Donald Kessler in 1978, this describes a scenario where the density of objects (satellites and debris) in LEO is high enough that collisions between objects could cause a cascade in which each collision generates space debris that increases the likelihood of further collisions and an exponential growth of debris. One implication is that the distribution of debris in orbit could render space activities and the use of satellites in specific orbital ranges difficult for many generations.

REUTERS/JOE SKIPPER

Outer Space Affairs (UNOOSA), governs much of the activity taking place in space. However, few effective governance tools have emerged in recent years to reflect new realities, such as the pressing need for an authority to govern satellite launches and servicing, space traffic control and common enforcement principles.[20]

As an exemplar challenge, the 1972 Space Liability Convention—which governs international responsibility for space objects launched from Earth—lacks precision around hybrid aircraft and rocket transport systems. For example, different legal authorities may govern depending on whether a vehicle is deemed to have launched when an aircraft takes off with a rocket attached or when the rocket detaches from the aircraft—and whether the hybrid vehicle is an aircraft or spacecraft while both pieces are attached. New addenda may be needed to clarify when space law should supersede aviation law.[21] Even the most robust governance realm, electromagnetic spectrum management, which is governed by the International Telecommunication Union (ITU), faces serious crowding pressures with new satellite systems and increased competition in the terrestrial spectrum usage of emerging 5G technologies.[22]

Respondents to the Global Risks Perception Survey (GRPS) reflect these gaps: 76% of respondents characterized the current state of international risk mitigation efforts in space as either "not started" or in "early development".

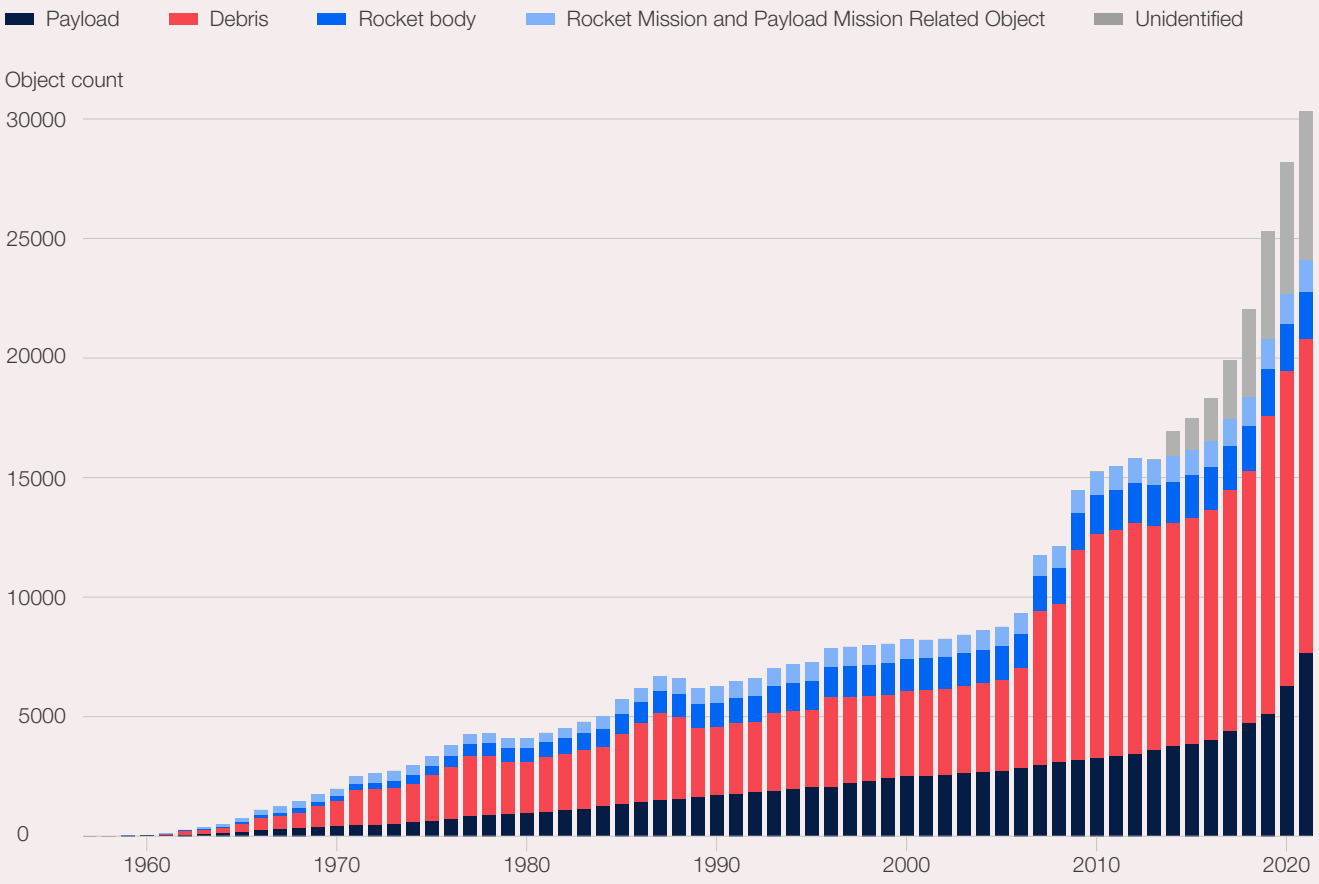
Governments, too, have developed their own national space policies,[23] with commercial interests as a key pillar of their national strategies, alongside national security and civil space policy. Although many governments have cooperated behind the scenes historically and still do today,[24] there is significant policy divergence among the 28 nations with space regulation,[25] and countries now operate at different scales and with different levels of ambition.[26] Such fragmentation compromises the further development of beneficial commercial space activities, which require shared norms across states to be able to function.[27]

National space ambitions also bring a growing risk of the militarization of space. The US military created a Space Force as a separate branch of its armed services in 2019, while Japan's Space Operations Squadron and the United Kingdom's

National space ambitions bring a growing risk of militarization of space

FIGURE 5.2

Evolution of the Number of Objects in All Orbits, 1960–2020



Source: European Space Agency. 2021. ESA's Annual Space Environment Report. 27 May 2021. https://www.sdo.esoc.esa.int/environment_report/Space_Environment_Report_latest.pdf

Space Command were both created in the last two years. Other leading armed forces also now typically include a space component—for instance, in 2021, the French Air Force became the Air and Space Force (Armée de l'Air & de l'Espace). In November of 2021, an anti-satellite weapons test conducted by Russia created significant debris and threatened astronauts on the ISS.[28] Other countries have conducted similar testing, raising the spectre of repeat occurrences from other nations, which would add considerably to the problem of space debris (see Figure 5.2).[29] A hypersonic weapons arms race also risks contributing to the militarization of space—China, Russia and the United States are all developing such weapons and each tested them in the second half of 2021.[30] And with expanding geospatial intelligence, all of Earth is observable by satellites, which could spur some nations to blind, jam or otherwise interfere with satellite Earth observation.[31] As technology advances, space mineral exploitation—already heralded as part of some deep-space exploration programmes—could also be viewed as another competitive wedge over a more distant horizon.[32]

Gaps in space governance render arms races even more likely. For example, the Outer Space Treaty prohibits nuclear weapons in space but does not address conventional weapons, which is particularly worrisome in today's context of conventional weapons development and testing in space. New rules are unlikely in the near future, as there is little agreement over key issues such as

boundaries, control over space objects, or dual-use systems.[33] Any further decline in cooperation on space governance will only exacerbate risks.[34]

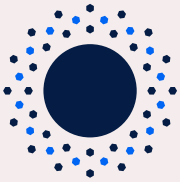
Service disruption and environmental unknowns: Consequences for people
Societies are dependent on space infrastructure in myriad everyday ways. GPS satellites not only allow for safe navigation in the air, land and sea, but they also underpin financial transactions, data transmissions and energy control systems. Threats—such as a massive solar storm or jamming or spoofing of GPS satellites—could cause the internet to slow, navigation systems to fail, and controls for energy grids, water or transportation to crash. Ripple effects across societies could be extensive, even for a few seconds of disruption.[35]

There are also significant unknowns about the impacts of rapid space development on Earth's environment—including damage to the ozone layer, butterfly effects from black carbon (soot) emissions, and possible alterations of the polar jet stream.[36] Of course, technological advances, such as developments in space-based solar power, could offset many of the potential negative environmental impacts of growing space exploration and exploitation.[37]

Gravitational push and pull: Consequences for governments
Notwithstanding high levels of private sector investment, increased commercialization and growing geopolitical competition will demand higher government spending on space programmes and defence at a time when public finances are under greater pressure due to the economic overhang of COVID-19 (see Chapter 1). For example, governments will increasingly need to compete for talent, with private sector entities offering more lucrative employment packages. Defence agencies will need to continue to expend resources to defend against more-sophisticated space-based weaponry and increasingly effective space-based tools of statecraft, such as enhanced surveillance or espionage.

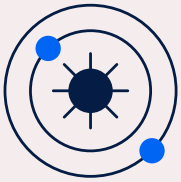
Yet, for a large majority of governments, space technology and access will remain out of reach altogether at a time when reliance on space technologies is growing for all. Forty-one nations have registered space agencies with UNOOSA,[38] yet the many governments not represented will continue to struggle to develop their capacities or earn a seat at the table in key decision-making processes. Without concerted effort to facilitate inclusive growth in the space realm, inequalities in the commercial and geopolitical benefits accruing from space development will only grow.

Shocks to Reflect Upon



Kessler Collapse

What if a cascading chain of collisions between near-Earth objects and space debris result in a saturated Low Earth Orbit that renders space practically unusable for further commercial development?



Solar Disruption

What if a massive solar event or geomagnetic storm disrupts satellite-based services and functions, causing massive, cascading economic and societal consequences on Earth?[39]

Property in Space

What if violations of the Outer Space Treaty—such as mineral resources being claimed in a Moon "gold rush"—are carried out without meaningful consequences?

Opportunity blocks: Consequences for businesses

Venture financing flooded into the space industry following the successful launches of commercial space flights. As commercial activity in space grows, more companies could crop up seeking entry while investor interest is high. However, if manufacturing, tourism or other space ventures fail to take flight, speculators and space industry companies could see their bubble burst. Similarly, grassroots campaigns to ban space pollution and prevent privatization of important science data could give investors pause, stifling the unmitigated venture financing in the field. [40]

Towards cooperation in space

Although space represents yet another realm in which geopolitical and commercial tensions will play out, important traditions of cooperation in this arena should not be forgotten. Norms of behaviour established through voluntary measures that are not legally binding with the goal of building trust and establishing mutual understanding have helped mitigate escalating tensions in the past. While this trend could continue, more robust formal governance will be required in a more crowded and competitive space. Specific and functional bilateral or multilateral agreements between major space powers could help create norms and influence broader global behaviours.

Space situational awareness, space traffic management and debris mitigation are areas in which norms-based and eventually formal international agreements would benefit all actors. Critically, and like other realms where technology is developing at a faster pace than its regulation, bringing private sector actors into the agreement processes will help ensure that such pacts reflect both commercial and technical realities. Taking advantage of these opportunities to achieve widely accepted norms could then help facilitate discussions around more challenging issues in space, such as limits on weaponization, ownership and appropriate venues from which to govern the realm.

REUTERS/ROSCOSMOS

Endnotes

1 Fildes, N. 2021. "Satellite groups face race to scale up or become space junk: Billionaire enthusiasts and new technology have brought valuations down to earth in a fragmented market". Financial Times. 14 November 2021. https://www.ft.com/content/138b3f58-cdad-484f-b180-ce0b96bb7028

2 Morgan Stanley. 2020 "Space: Investing in the Final Frontier". 24 July 2020. https://www.morganstanley.com/ideas/investing-in-space; Stutt, A. 2020. "The global race to mine outer space". Mining.com. 22 May 2020. https://www.mining.com/the-global-race-to-mine-outer-space/; Woo, E. 2021. "Start-ups aim beyond Earth". The New York Times. 7 July 2021. https://www.nytimes.com/2021/07/07/technology/space-start-ups.html

3 Morgan Stanley. 2020. Op. cit.

4 Gabbat, A. 2021. "US accuses Russia of 'dangerous' behavior after anti-satellite weapons test". The Guardian. 15 November 2021. https://www.theguardian.com/science/2021/nov/15/us-investigating-debris-event-space-reports-russia-anti-satellite-weapon-test; Jones, A. 2021. "China's Tiangong space station". Space. 24 August 2021. https://www.space.com/tiangong-space-station; Rome, N. 2021. "Growth of space and lunar stations: Promise amidst geopolitical risk". Georgetown Security Studies Review. 14 July 2021. https://georgetownsecuritystudiesreview.org/2021/07/14/growth-of-space-and-lunar-stations-promise-amidst-geopolitical-risk/

5 Rome. 2021. Op. cit.

6 NASA. 2021. Artemis Mission. https://www.nasa.gov/specials/artemis/

7 European Space Policy Institute. 2021. Emerging Spacefaring Nations. June 2021. https://espi.or.at/publications/espi-public-reports/category/2-public-espi-reports; Goswami, N. 2021. "Status of existing and emerging Asia-Pacific space powers capabilities". Nautilus Institute. 20 August 2021. https://nautilus.org/napsnet/napsnet-special-reports/status-of-existing-and-emerging-asia-pacific-space-powers-capabilities/

8 Buchs, R. 2021. "Intensifying space activity calls for increased scrutiny of risks". EPFL. 14 April 2021. https://www.epfl.ch/research/domains/irgc/spotlight-on-risk-series/intensifying-space-activity-calls-for-increased-scrutiny-of-risks/

9 Ibid.

10 Davis, G. 2021. "SpaceX's competitors claim Elon Musk could monopolize space". Tech Times. 29 May 2021. https://www.techtimes.com/articles/260823/20210529/spacexs-competitors-claims-elon-musk-monopolize-space-starlink-constellation-unsustainable.htm

11 Broad, W.J. 2021. "How space became the next 'great power' contest between the U.S. and China". The New York Times. 6 May 2021. https://www.nytimes.com/2021/01/24/us/politics/trump-biden-pentagon-space-missiles-satellite.html

12 Daehnick, C. and Harrington, J. 2021. "Look out below: What will happen to the space debris in orbit?" McKinsey & Company. 1 October 2021. https://www.mckinsey.com/industries/aerospace-and-defense/our-insights/look-out-below-what-will-happen-to-the-space-debris-in-orbit; Jones, A. 2021. "China is developing plans for a 13,000-satellite megaconstellation". SpaceNews. 21 April 2021. https://spacenews.com/china-is-developing-plans-for-a-13000-satellite-communications-megaconstellation/; Spiegel Business. 2021. "Bezos' space company is planning a private space station – slightly smaller than the ISS". Spiegel Business. 25 October 2021. https://www.spiegel.de/wirtschaft/unternehmen/jeff-bezos-plant-private-raumstation-orbital-reef-etwas-kleiner-als-die-iss-a-1779efd7-6ee6-4c92-9986-7fc996951e8f

13 Daehnick, C. and Harrington, J. 2021. "Look out below: What will happen to the space debris in orbit?" McKinsey & Company. 1 October 2021. https://www.mckinsey.com/industries/aerospace-and-defense/our-insights/look-out-below-what-will-happen-to-the-space-debris-in-orbit

14 NASA. 2021. State-of-the-Art Small Spacecraft Technology. October 2021. https://www.nasa.gov/sites/default/files/atoms/files/soa_2021.pdf

15 Nature. 2021. "The world must cooperate to avoid a catastrophic space collision". Nature. 11 August 2021. https://www.nature.com/articles/d41586-021-02167-5

16 Strickland, A. 2021. "Space junk hit the International Space Station, damaging a robotic arm". CNN. 1 June 2021. https://edition.cnn.com/2021/06/01/world/iss-orbital-debris-robotic-arm-scn/index.html

17 Hyde, J. L., Christiansen, E.L. and Lear, D.M. 2019. "Observations of MMOD Impact Damages to the ISS". NASA. 9 December 2019. https://ntrs.nasa.gov/citations/20190033989; Kessler, DJ. and Cour-Palais, B.G. 1978. "Collision frequency of artificial satellites: The creation of a debris belt". Journal of Geophysical Research. Volume 83, Issue A6. 1 June 1978.

18 The European Space Agency. 2021. "Space debris by the numbers". 22 December 2021. https://www.esa.int/Safety_Security/Space_Debris/Space_debris_by_the_numbers

19 Rooney, K. 2021. "The big space clean-up – and why it matters". World Economic Forum Global Agenda. 20 May 2021. https://www.weforum.org/agenda/2021/05/space-junk-clean-satellite/

20 Stuart, J. 2017. "The Outer Space Treaty has been remarkably successful – but is it fit for the modern age?". The Conversation. 27 January 2017. https://theconversation.com/the-outer-space-treaty-has-been-remarkably-successful-but-is-it-fit-for-the-modern-age-71381; Kwan, R. and Henley, J. 2021. "China berates US after 'close encounters' with Elon Musk satellites". The Guardian. 28 December 2021. https://www.theguardian.com/science/2021/dec/28/china-complains-to-un-after-space-station-is-forced-to-move-to-avoid-starlink-satellites

21 Li, C. and Wang, G. 2021. "Applicability of the Liability Convention for Private Spaceflight". Space: Science & Technology. 4 May 2021. https://doi.org/10.34133/2021/9860584

22 Panhans, D., Schicht, R., Hamady, F. and Werlé, T. 2020. "The Coming Battle for Spectrum". 11 February 2020. https://www.bcg.com/en-us/publications/2020/coming-battle-for-spectrum

23 See, e.g., U.S. Office of the Vice-President. 2021. "United States Space Priorities Framework." 1 December 2021. https://www.whitehouse.gov/wp-content/uploads/2021/12/United-States-Space-Priorities-Framework-_-December-1-2021.pdf

24 Marshall W. and Hadfield, C. 2021. "Why the U.S. and China should collaborate in space". Time. 15 April 2021. https://time.com/5954941/u-s-china-should-collaborate-in-space/; Shackelford, S. 2019. "Renewed space rivalry between nations

ignores a tradition of cooperation". The Conversation. 10 January 2019. https://theconversation.com/renewed-space-rivalry-between-nations-ignores-a-tradition-of-cooperation-108810

25 Goguichvili, S., Linenberger, A. and Gillette, A. 2021. "The Global Legal Landscape of Space: Who Writes the Rules on the Final Frontier?" 1 October 2021. https://www.wilsoncenter.org/article/global-legal-landscape-space-who-writes-rules-final-frontier

26 European Space Policy Institute. 2021. "Emerging Spacefaring Nations". June 2021. https://espi.or.at/publications/espi-public-reports/category/2-public-espi-reports

27 Goguichvili, Linenberger and Gillette. 2021. Op. cit.

28 Gabbat, A. 2021. "US accuses Russia of 'dangerous' behavior after anti-satellite weapons test". The Guardian. 15 November 2021. https://www.theguardian.com/science/2021/nov/15/us-investigating-debris-event-space-reports-russia-anti-satellite-weapon-test; Rincon, P. and Amos, J. 2021. "Russian anti-satellite test adds to worsening problem of space debris". BBC. 16 November 2021. https://www.bbc.com/news/science-environment-59307862

29 Historically, collisions and anti-satellite weapons testing have created significant increases in the number of orbiting space objects and debris, e.g., in 2009, when an active commercial communications satellite collided with a derelict military satellite, or in 2007, from an anti-satellite test.

30 Sevastopulo, D. and Hille, K. 2021. "China tests new space capability with hypersonic missile". Financial Times. 16 October 2021. https://www.ft.com/content/ba0a3cde-719b-4040-93cb-a486e1f843fb; Stone, M. 2021. "U.S. in hypersonic weapon 'arms race' with China -Air Force secretary". Reuters. 1 December 2021. https://www.reuters.com/business/aerospace-defense/us-hypersonic-weapon-arms-race-with-china-air-force-secretary-2021-11-30/; Reuters. 2021. "Russia conducts test launch of hypersonic missile -Interfax". 24 December 2021. https://www.reuters.com/world/europe/russia-conducts-test-launch-hypersonic-missile-interfax-2021-12-24/

31 Vinci, A. 2020. "The coming revolution in intelligence affairs". Foreign Affairs. 31 August 2020. https://www.foreignaffairs.com/articles/north-america/2020-08-31/coming-revolution-intelligence-affairs

32 Stutt, A. 2020. "The global race to mine outer space". Mining.com. 22 May 2020. https://www.mining.com/the-global-race-to-mine-outer-space/

33 Pozdnyakova, G. 2021. "Top-10 themes for 2022: Space: a worrying geopolitical frontier". Deutsch Bank. 8 December 2021. https://www.dbresearch.com/servlet/reweb2.ReWEB?rwsite=RPS_EN-PROD&rwobj=ReDisplay.Start.class&document=PROD0000000000521006

34 Panda, A. 2021. "Military Competition, New Technologies, and Space". An Asian Space Odyssey. March 2021. Diplomat Risk Intelligence. https://dri.thediplomat.com/report/2021-03/

35 Scott, C. 2018. "The violent solar storms that threaten Earth". BBC. 22 November 2018. https://www.bbc.com/news/science-environment-46260959; Tullis, P. 2019. "GPS is easy to hack, and the U.S. has no back-up". Scientific American. 1 December 2019. https://www.scientificamerican.com/article/gps-is-easy-to-hack-and-the-u-s-has-no-backup/

36 Ross, M. and Vedda, J.A. 2018. "The Policy and Science of Rocket Emissions". Center for Space Policy and Strategy. 31 March 2018. https://aerospace.org/sites/default/files/2018-05/RocketEmissions_0.pdf

37 David, L. 2021. "Space solar power's time may finally be coming". Space.com. 3 November 2021. https://www.space.com/space-solar-power-research-advances

38 UNOOSA (United Nations Office for Outer Space Affairs). https://www.unoosa.org/oosa/en/ourwork/space-agencies.html, accessed 15 December 2021

39 Khodairy, S., Sharaf, M., Awad, M., Hamed, R.A. and Hussein, M. 2020. "Impact of solar activity on Low Earth Orbiting satellites'. Journal of Physics: Conference Series 1523 (1): 012010. IOP Publishing. https://iopscience.iop.org/article/10.1088/1742-6596/1523/1/012010/pdf

40 Szkutak, R. 2021. "The billionaire space race launches a new venture capital solar system". Forbes. 16 September 2021. https://www.forbes.com/sites/rebeccaszkutak/2021/09/16/the-billionaire-space-race-launches-a-new-venture-capital-solar-system/?sh=74f837e7482e

CHAPTER 6

Refreshing Resilience

COVID-19 Lessons for a Whole-of-Society Response

67.2%

COVID-19-vaccinated population in high-income countries

20-40×

increase in number of daily COVID-19 cases between peak and trough

2.1 million

maximum estimated excess deaths in Africa by 2021

REUTERS/SEBASTIAN CASTANEDA

Adaptive resilience to the pandemic at the national level

The 2021 *Global Risks Report* closed with a reflection on the extent to which shortcomings in the pandemic response could be attributed to long-standing complacencies, the novel and specific complexities of COVID-19, the volatile and divisive (geo)political environment or simple mismanagement. This chapter takes stock of national response strategies implemented in the second year of the pandemic, and then reflects on collaborative opportunities within countries to improve preparedness for future crises and organizational resilience.

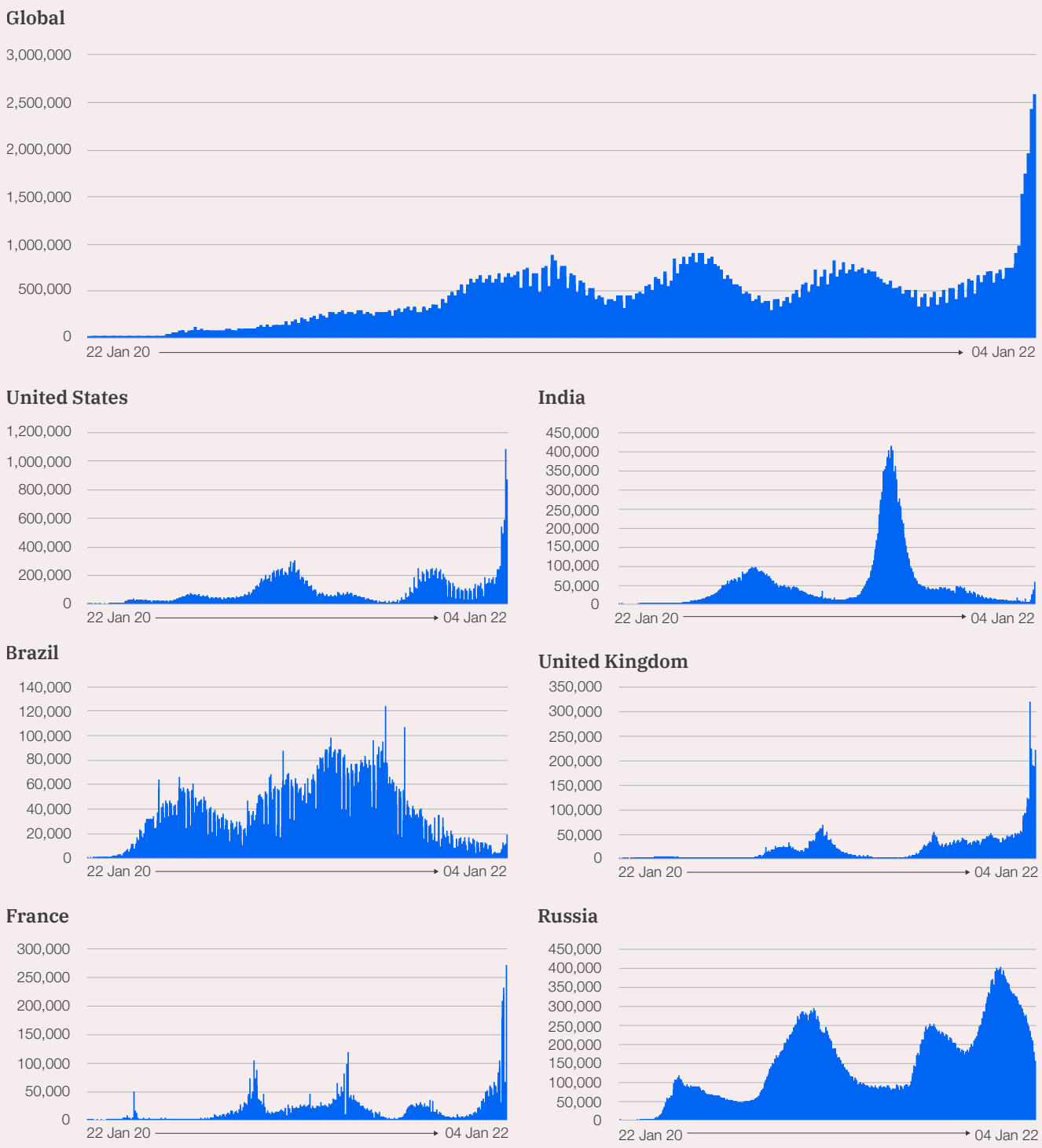
During 2020, national governments sought to protect lives and livelihoods against a novel virus that was resulting in a significant mortality rate—with the backdrop of significant shortcomings in national and global preparedness. In 2021, as the virus evolved more contagious variants, governments sought to deploy new responses, in alignment with measures developed the previous year, to return to societal and economic normalcy. Most countries experienced several surges during the year, with the number of daily cases characterized by exponential growth and a 20- to 40-fold increase between peak and trough (see Figure 6.1). By this measure, most countries presented both success stories and cautionary tales at different times.

Most countries saw both success stories and cautionary tales at different times

REUTERS/ELOISA LOPEZ

FIGURE 6.1

COVID-19 Daily New Cases: Global and Top Six Countries by Infections



Source: Worldometer. Covid-19 Coronavirus Pandemic – "Daily new cases". https://www.worldometers.info/coronavirus/, accessed 5 January 2022.

Two interlinked factors have proved critical for the effective national management of the pandemic: first, governments' readiness to adjust response strategies according to changing circumstances; and second, their ability to maintain societal trust and compliance through principles-based decisions and effective communications.

Flexible response strategies

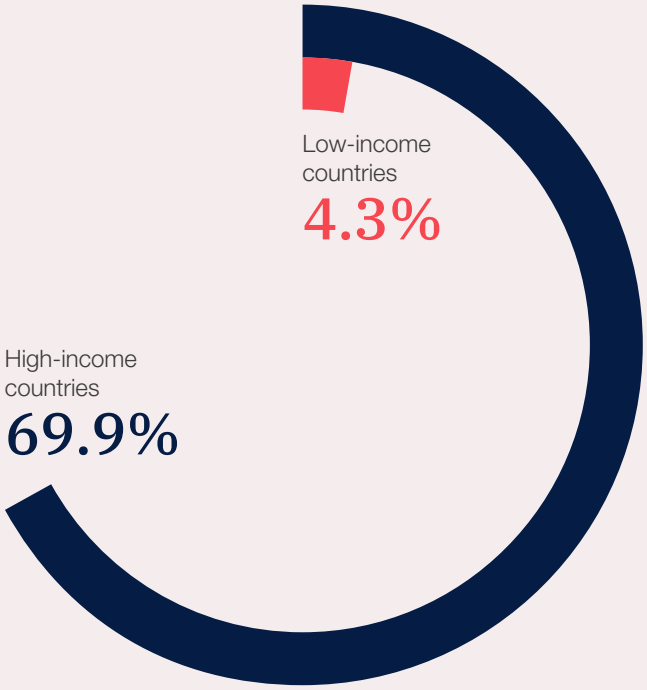
In general, effective national responses were characterized by a holistic view of societal well-being, multi-pronged approaches to transmission control and health system protection, robust coordination of policy and process, reliable logistics and the deployment of new interventions and increasingly granular and real-time data where available. Countries such as Chile and Finland were better able to manage peak periods than those with less well-rounded approaches.[1] They achieved this via cross-departmental policy agendas; expanded networks of community health workers; key health worker protections; a range of individually imperfect but collectively effective transmission control measures such as testing, tracing, and isolating; digital healthcare technologies; and early investment in anticipation of future needs.

Critical for many countries was the establishment of well-judged policy transitions between enabling social interaction and economic activity when possible and returning, when needed, to the kind of mobility constraints that were default strategies in the early stages of the crisis. Rapid and wholesale easing of constraints on social and economic activity often resulted in a steep rise in case numbers, although the impact on health systems and mortality was often mitigated by high vaccination rates. Some countries that had prided themselves on very low case numbers for a long time found it hard to acknowledge or pivot when that was no longer the best indicator to measure the state of the pandemic.[2] The Omicron variant, with its higher infectiousness, will moreover force governments to revisit the balance between sustaining economic activity and limiting spread. Some are choosing to minimize disruptions in light of the virus' evidently milder threat, although they must be prepared to reinstate restrictions as necessary given that healthcare systems remain at risk of collapse.[3]

The arrival of effective vaccines and antiviral treatments changed the game in terms of managing the impact of the virus on citizens' health and national health systems, enabling greater latitude in other policies.[4] Mass deployment of affordable rapid tests also helped people move and mingle again while mitigating transmission risk. However, although a range of vaccines was technically available from early in the year, differing negotiating powers, contracting approaches and approval regimes had a strong impact on programme rollout timetables. Many high-income countries had privileged access to vaccines: by early December 2021, all but three Organisation for Economic Co-operation and Development (OECD) countries had double-vaccinated at least 50% of their populations.[5] Some middle-income countries had also achieved high levels of vaccination: for example, the 79% vaccination rate in Malaysia was largely due to effective distribution,[6] while Brazil's 65% was attributed to strong vaccine enthusiasm.[7]

FIGURE 6.2

Percentage of the Population Who Are Fully Vaccinated



Source: ONE. 2021. "Data dive: The astoundingly unequal vaccine rollout". January 2022.

REUTERS/ELOISA LOPEZ

The lowest vaccination rates were mostly found in low-income countries (see Figure 6.2), especially in Africa, that had to rely on "vaccine diplomacy" initiatives from individual countries and multilateral agreements such as the Covid-19 Vaccines Global Access (COVAX) programme. The latter suffered from low contributions from high-income countries, high levels of bureaucracy, unpredictable supplies, and storage and distribution challenges.[8] Relatively younger populations and "a favorable climate may have blunted the mortality of the virus in these countries, though excess deaths were estimated at between 0–2.1 million in Africa by May 2021,[9] and long Covid may emerge as a longer-term challenge given the large number of non-fatal cases.

In general, successful vaccine rollout programmes struck a balance between speed and robustness, recognizing that perfect was sometimes the enemy of good. Vaccine effectiveness was found to improve following a second dose but waned over time, leading advanced economies to introduce booster jab programmes in which take-up and speed were key priorities.[10] By the latter part of the year, analysis showed that fully vaccinated individuals were less likely to transmit the virus, experience severe or long-haul symptoms, occupy hospital beds or die.[11]

Although global eradication of COVID-19 is no longer a viable option, persistent transmission of SARS-Cov-2 allows the emergence of new variants that are more contagious and may be more virulent and escape immunity conferred by infection or existing vaccines. Hence, the relatively slower vaccine rollouts in middle- and low-income countries, as well as vaccine hesitancy wherever present, remain a continued pandemic risk for all countries and require anticipation of further policy transitions. As and when new variants arise, governments will need to reimpose an appropriate set of control measures.

Maintaining societal trust

Maintaining societal trust involved galvanizing compliance and cooperation across citizens and the business community through frequent changes of government policy over an extended period. This often proved

Mass and affordable testing helped people move and mingle while mitigating transmission

challenging as, during 2021, many citizens became even more weary of lockdowns and obligations such as mask-wearing. In late November, several European countries and Australia experienced riots when governments tightened regimes in the face of ballooning case numbers.[12]

Moreover, in advanced economies with widespread access to vaccines, significant percentages of the adult population remained unvaccinated at the end of 2021 due to misplaced concerns about the risk of the vaccines relative to that of catching the virus, over-confidence in their own natural immunity and adherence to a range of theories that lack scientific basis.[13] In other countries, general distrust of the government has resulted in widespread vaccine hesitancy, with alternative sources of authority, including local opinion and religious leaders, not sufficiently able to help allay fears.[14]

The trust component of managing this crisis has often depended on a balance between imposing constraints or coercions based on science and policies that encourage good behaviour. Communication has needed to steer a narrow course between individual freedoms and collective resilience; indeed, nearly 50% of the World Economic Forum global risk experts identified this tension as one of the most critical for societies to manage.[15] The challenge will only intensify as the pandemic extends into its third year and the public grows increasingly weary, especially during festive seasons as expectations for unfettered social activity increase.

The faster distribution of testing kits, along with easier self-administration and greater reliability of results, were helpful for enabling social interactions and international mobility. Widespread availability of affordable testing will be crucial as restrictions are increasingly lifted and greater social activity causes demand to outstrip supply, as has already been seen in some countries. However, regarding vaccines, some governments have become concerned that voluntary measures have reached their limits, especially with the arrival of the Omicron variant.[16] Plans for vaccination requirements, with sanctions on employment or mobility for those who continue to resist, will test societal goodwill and compliance as well as government determination in light of divisive politics.[17] Additionally, national resilience strategies for future pandemics may require anticipation of some level of distrust and defiance of restrictions and interventions aimed at protecting vulnerable population segments.

REUTERS/HANNIBAL HANSCHKE

Preparing national resilience ecosystems for future crises

The COVID-19 crisis repeatedly surprised those charged with anticipating its trajectory and will likely leave further complex problems in its wake. Nor is the pandemic and its response the only challenge that governments, societies and businesses are facing. As the *Global Risks Report* sets out, new crises may lie just over the horizon.

Many critical risks demand a whole-of-society response. This involves not only the engagement of different sectors leading to multiple individual actions, but also more effective interaction between different sectors in ways that are accretive to well-being and prosperity.[18]

Countries must distinguish between different resilience goals to harness their collective capabilities more effectively and navigate the many inevitable trade-offs, as failure to appreciate where agendas are misaligned will limit the traction any solutions can gain. One such goal might be community resilience to potential disasters; another might be reliable critical economic and societal infrastructure; a third might be long-term strategic imperatives such as industrial transformation.[19] Each of these goals requires different strategies, providing a frame for different cross-sectoral interactions.

Government lens

National risk assessments and resilience strategy reviews should be used to reveal where momentum is insufficient and greater government intervention is needed. It is not desirable or feasible for governments to seek to fill all gaps themselves: instead, they should look to harness the capabilities and energies of other sectors to complement enhanced competencies that ought to lie in the public realm.[20] Strategies should set out what is needed and examine all available levers with fresh eyes. They should identify where governments may need to compel action by others, and where they can exercise power as a client, stimulate new initiatives, facilitate collaboration or simply act as cheerleader for good practices.

In their interactions with the private sector, governments that are more dirigiste might want to adjust their approaches to models for stockpiling critical goods, requisitioning and procurement in a crisis.[21] All might also seek tougher cybersecurity mandates and set out stronger expectations of stress testing for critical infrastructure.[22] They might seek to bring about a research and development ecosystem for resilience, coordinate crisis management exercises involving public and private sectors and provide a level of backstop for pooled insurance schemes targeted at catastrophic risks.[23]

On three issues, finding a balanced path is critical. First, it is essential to allocate risk in a way that means the taxpayer does not ultimately pay up in every crisis nor do governments sweep risks off the public balance sheet onto the private sector. More transparent, analysis-led discussions about risks and tolerances should spur more equitable, creative solutions about the cost and pricing of risk as well as fiscal and market buffers that might mitigate fallout in the event of crisis.

Second, regulating for resilience must factor in rapid changes in assets, industries and systems; conflicting priorities in regulatory mandates; and enforcement challenges. Arguably, systemically important assets, firms and sub-sectors ought to experience greater oversight to prevent "hidden" assets in digital ecosystems, dominant firms in niche but critical industries and growing segments of certain sectors

Government should harness capabilities in other sectors to enhance public competencies

where the plausible near-simultaneous failure of several providers could have negative far-reaching consequences.[24] For regulatory regimes that primarily look out for present-day consumers, long-term resilience should be a central tenet and capability underpinning the development and implementation of major critical infrastructure capital investment plans.[25] Stronger cross-sector regulatory hubs could sharpen debate and help reconcile differing agendas of bodies with separate statutory powers.[26]

Third, data-sharing arrangements must be adjusted in a way that enables both pre-emptive resilience building and sharper crisis management. There are good reasons for constraining some flows of data and intelligence, including national security, commercial confidentiality, antitrust constraints and personal privacy. Acknowledging this, governments may seek to identify crisis circumstances—such as a cybersecurity lapse—in which they should compel critical infrastructure operators to provide data to government bodies. In other situations, such as an earthquake, they might permit, or even encourage, competing firms to share data with each other to ensure strategic supplies for the nation. Prior to crises, governments should consider how to develop more collaborative approaches to scenario and impact analyses, build semi-accessible and proprietary data into resilience analytics and crisis decision-making, and better facilitate pre-competitive data sharing by companies for innovations that will benefit both participants and the national good.[27]

Business lens

Many companies have sought to understand how they can contribute to the resilience of the countries in which they operate. They recognize that better national-level preparedness leads to shock events having smaller impacts on the economy and stability of government policy, creating a better environment in which to plan, invest and execute.

Opportunities fall into four groups. First, large firms already look intensively at business interruption risks across supply chains, managed service providers, utilities and customers with a view to softening the impact of bottlenecks and outages; smaller firms could do the same with a lighter touch.[28] Second, nationally important companies worked with each other where permitted during the pandemic; more broadly scoped codes of conduct could set out best-practice behaviours per industry for future crises.[29] Third, the pandemic spurred companies to look harder at the resilience of their workforces and the communities in which they are located; large employers could build a resilience dimension into health and benefits offerings.[30] Fourth, some firms have been seeking to take a more

GETTY/VCG

GETTY

active role in addressing large-scale public policy challenges that affect their business but cannot be resolved by government alone; more of that effort could be directly positioned in support of public goods.[31]

While public funds have traditionally directed resilience efforts, there is a growing imperative for businesses to take up the mantle of driving innovation in order to reduce blind spots and counter stovepiping tendencies within government. Greater private sector participation in strategic forums can allow experts and practitioners to contribute to and challenge government agendas. Dynamic cross-sectoral interactions around priorities, policies and operating practices can also help uncover efficient and efficacious solutions as well as generate broader traction for fresh initiatives.[32]

Community lens

Both the pandemic and extreme weather events have highlighted areas where central governments and local bodies can combine more effectively. Failure to join up policy agendas across national government departments can have devastating impacts at the local level, where crises play out and disconnects are exposed. Similarly, "air gaps" between central and local governments—often due to struggles for authority or weaknesses in liaison networks—have compromised data flows, the effectiveness of initiatives and local trust.[33] Improved communication processes, better devolution of decision-making authorities, stronger coordination of on-the-ground efforts between central government specialist agencies and local administrations and better capacity-building at local and national levels would go a long way in supporting resilience.

Better national preparedness creates a better environment to invest

There is scope for central and local governments to do more to support resilience efforts at the community level, often in partnership with non-governmental organizations and businesses. Local resilience forums can galvanize communities to provide detailed intelligence on situational vulnerabilities and likely impacts of key risks, helping to prioritize resilience measures. Enhancing awareness and participation, empowering local actors and building capabilities are vital for the cultural shift that is essential for sustaining resilience programmes over the long term.

There are multiple opportunities to enrich interfaces between academic communities and government agendas at local, national and international levels, especially for the provision of expertise and evidence on matters of science and technology.[34] Collaborative exploration of risk and resilience issues—before, during and after a crisis—would benefit from stronger, more flexible communication channels and higher levels of trust (see Box 6.1).

BOX 6.1

From Insights to Practice

Based on the challenges of the past year, the World Economic Forum has worked with two of its principal risk communities, the Chief Risk Officers Community and the Global Future Council on Frontier Risks, to identify five practical lessons to improve organizational practice for resilience:

1. **Ground analyses in delivery requirements.**

It is often useful to start not with specific risks but with the types of failure, damage and attrition that could compromise core business goals. Working back from these undesirable outcomes makes for a more open assessment of current practices and a better appreciation of the capabilities, levers, tools and processes that might need to be introduced, deployed, redesigned or enhanced.

2. **Appreciate vulnerabilities within the broader ecosystem.**

As well as examining the critical assets and operations they control, organizations should look at the broader ecosystem in which they operate. They should examine their resilience to shortfalls, outages and delays of the third-party assets and services on which they depend, and the tolerances of those who depend on them.

3. **Embrace a diversity of resilience strategies.**

Some possible crises can be mitigated by placing more emphasis on just-in-case reliability than on just-in-time efficiency. Others may be best served by implementing back-ups and redundancies, adjusting operational processes, or ensuring that the organization can move quickly and adapt in order to maintain business continuity. Supportive employee behaviours are as vital as structural measures, especially when empowered by good leadership and effective communication.

4. **Connect resilience efforts with other goals.**

Many organizational environmental, social and governance (ESG) goals are shared with a broad-based resilience platform and would benefit from improved alignment. For example, shortening supply chains can advance net zero strategies as well as reduce exposure to adverse geoeconomic developments, while strong community relations may help recovery initiatives in the event of a disaster.

5. **Consider resilience to be a journey not a destination.**

Organizations with leading resilience programmes learn from stress-testing exercises and actual crises to emerge stronger, more supple and better prepared. They are alert to changing circumstances that may demonstrate elevated risks, vigilant in challenging themselves about blind spots and shortcomings that require additional action and eager to adapt response strategies to better achieve critical goals.

Endnotes

1 Bloomberg. 2021. "The Best and Worst Places to Be as Winter Meets Omicron". 30 November 2021. https://www.bloomberg.com/graphics/covid-resilience-ranking/

2 Tan, Y. 2021. "What went wrong in Singapore and Taiwan?" BBC News. 20 May 2021. https://www.bbc.com/news/world-asia-57153195

3 The Guardian. 2021. "WHO warns Omicron could overwhelm health systems as cases rise to record highs in Europe". 29 December 2021. https://www.theguardian.com/world/2021/dec/29/who-warns-omicron-could-overwhelm-health-systems-as-cases-rise-to-record-highs-in-europe

4 Crow, D. 2021. "How mRNA became a vaccine game-changer". Financial Times. 13 May 2021. https://www.ft.com/content/b2978026-4bc2-439c-a561-a1972eeba940

5 Our World in Data. Share of the population fully vaccinated against COVID-19. https://github.com/owid/covid-19-data/tree/master/public/data, accessed 15 December 2021.

6 Kurlantzick, J. 2021. "Lessons ASEAN could learn from Malaysia's pandemic success". The Japan Times. 5 November 2021. https://www.japantimes.co.jp/opinion/2021/11/05/commentary/world-commentary/malaysias-pandemic-success/

7 Freelon, K. 2021. "In Brazil's successful vaccine campaign, a lesson for the U.S." Undark Magazine. 14 October 2021. https://undark.org/2021/10/14/in-brazil-successful-vaccine-campaign-lesson-for-us/

8 Fleming, S., Mancini, P.D. and Pilling, D. 2021. "'Erratic' European Covid vaccine donations hamper African jabs rollout". Financial Times. 9 December 2021. https://www.ft.com/content/d0b53ea4-5eef-4bc7-814c-a69b0dfa1c06

9 The Economist. 2021. "There have been 7m-13m excess deaths worldwide during the pandemic". The Economist. 15 May 2021. https://www.economist.com/briefing/2021/05/15/there-have-been-7m-13m-excess-deaths-worldwide-during-the-pandemic

10 Stieg, C. 2021. "New data says you should get a Covid vaccine booster shot as soon as you're eligible — here's why". CNBC. 10 November 2021. https://www.cnbc.com/2021/11/10/why-young-healthy-people-should-get-covid-vaccine-booster-shots.html

11 Aravindan, A and Lin, C. 2021. "Vaccinated people make up 75% of recent COVID-19 cases in Singapore, but few fall ill". Reuters. 23 July 2021. https://www.reuters.com/world/asia-pacific/vaccinated-people-singapore-make-up-three-quarters-recent-covid-19-cases-2021-07-23/; Mathieu, E. and Roser, M. 2021. "How do death rates from COVID-19 differ between people who are vaccinated and those who are not?" Our World in Data. 23 November 2021; updated 10 December 2021. https://ourworldindata.org/covid-deaths-by-vaccination

12 DW. 2021. "COVID curbs spark protests worldwide". Deustche Welle. 21 November 2021. https://www.dw.com/en/covid-curbs-spark-protests-worldwide/a-59892484

13 See, e.g., Thompson, D. 2021. "Millions are saying no to the vaccines. What are they thinking?" The Atlantic. 4 May 2021. https://www.theatlantic.com/ideas/archive/2021/05/the-people-who-wont-get-the-vaccine/618765/; Calonzo, A. and Tan, K. 2021."Anti-Vaxxer Propaganda Spreads in Asia, Endangering Millions". Bloomberg. 1 July 2021. https://www.bloomberg.com/news/articles/2021-06-30/anti-vaxxer-disinformation-spreads-in-asia-endangering-millions

14 Hartwig, R. and Hoffmann, L. 2021. Challenging Trust in Government: COVID in Sub-Saharan Africa. GIGA Focus Afrika. https://www.giga-hamburg.de/en/publications/25196662-challenging-trust-government-covid-saharan-africa/

15 The World Economic Forum Chief Risk Officers Community and Global Future Council on Frontier Risks were asked which tension was most critical in achieving strong resilience in societies. In addition to "individual rights v. collective resilience", other selected tensions included "cost optimization v. risk exposure" (22%), "government overreach v. expectation management" (11%), "public v. private protocols in a crisis" (11%), and "use of emergency powers v. market evolution" (4%).

16 Onishi, N. and Casey, N. 2021. "Crack Down Hard, or Wait and See? Europe Splits on Omicron Response". The New York Times. 20 December 2021. https://www.nytimes.com/2021/12/20/world/europe/europe-divided-omicron-response.html

17 Fleming, S. and Chazan, G. 2021. "Von der Leyen calls for EU 'discussion' on mandatory vaccination". Financial Times. 1 December 2021. https://www.ft.com/content/3e96d309-0283-4a33-9fc0-2bc5de22cb5f; Henley, J. 2021. "Germany: Mandatory Covid jabs a step closer as unvaccinated face lockdown". The Guardian. 2 December 2021. https://www.theguardian.com/world/2021/dec/02/germany-could-make-covid-vaccination-mandatory-says-merkel; Shear, M. D. and Scheiber, N. 2021. "Biden tests limits of presidential power in pushing vaccinations". New York Times. 4 November 2021. https://www.nytimes.com/2021/09/10/us/politics/biden-vaccines.html

18 OECD (Organisation for Economic Co-operation and Development). 2014. Recommendation of the Council on the Governance of Critical Risks. https://www.oecd.org/gov/risk/recommendation-on-governance-of-critical-risks.htm

19 Smith-Bingham, R. 2021. Partnering with purpose: Strengthening national-level resilience in the UK through more dynamic public-private interactions. National Preparedness Commission & Marsh McLennan. https://www.marshmclennan.com/content/dam/mmc-web/insights/publications/2021/november/Marsh_McLennan-National_Preparedness_Commission_Partnering-with-Purpose_vF.pdf

20 OECD. 2018. Assessing Global Progress in the Governance of Critical Risks. OECD Reviews of Risk Management Policies. https://doi.org/10.1787/9789264309272-en

21 OECD. 2020. Stocktaking report on immediate public procurement and infrastructure responses to COVID-19. Updated 24 June. https://www.oecd.org/coronavirus/policy-responses/stocktaking-report-on-immediate-public-procurement-and-infrastructure-responses-to-covid-19-248d0646/#section-d1e2236

22 Caminiti, S. 2021. "What cybersecurity leaders say they need from the federal government". CNBC. 25 August 2021. https://www.cnbc.com/2021/08/25/what-cybersecurity-leaders-say-they-need-from-the-federal-government.html

23 EIOPA (European Insurance and Occupational Pensions Authority). 2021. "EIOPA staff paper on measures to improve the insurability of business interruption risk in light of pandemics". Luxembourg: Publications Office of the European Union. https://www.eiopa.europa.eu/sites/default/files/publications/eiopa-staff-paper-on-measures-to-improve-insurability.pdf

24 Smith-Bingham, R. 2021. Op. Cit

25 OECD. 2021. Building Resilience: New Strategies for Strengthening Infrastructure Resilience and Maintenance. https://www.oecd.org/g20/topics/infrastructure/Building-Infrastructure-Resilience-OECD-Report.pdf

26 Financial Services Regulatory Initiatives Forum. 2021. Regulatory Initiatives Grid. November 2021. https://www.fca.org.uk/publication/corporate/regulatory-intitiatives-grid-november-2021.pdf

27 World Economic Forum. 2021. "Data-Driven Economies: Foundations for Our Common Future". White Paper. April 2021. https://www3.weforum.org/docs/WEF_WP_DCPI_2021.pdf

28 Asseri, A. H., Abilkasimov, M., Frio, D. and Beato, F. 2021. "Managing third-party risks? Here's how a holistic approach can help". World Economic Forum Agenda. 30 September 2021. https://www.weforum.org/agenda/2021/09/managing-third-party-risks-heres-how-a-holistic-approach-can-help/

29 MedTech Europe. 2020. "MedTech Europe Code Guidance on COVID-19 Emergency Support". 27 March 2020. https://www.medtecheurope.org/wp-content/uploads/2020/03/MTE_code_guidance_compliance_covid19.pdf

30 Hariharan, K., Rudoy, J. and Friedman, L. 2021. "How businesses can improve the health of societies". BRINK. 13 July 2021. https://www.brinknews.com/how-businesses-can-improve-the-health-of-societies/

31 Rosenberg, S. and Fried, I. 2021. "The government-industry cyberdefense dance". Axios. 26 August 2021. https://www.axios.com/cybersecurity-summit-biden-government-industry-e8185e32-0346-40e5-af4f-6cd79f93cbb9.html

32 See, e.g., Zurich Insurance Group. 2021. "The Zurich Flood Resilience Alliance". https://floodresilience.net/zurich-flood-resilience-alliance/

33 Dilanian, K. and De Luce, D. 2020. "Trump administration's lack of a unified coronavirus strategy will cost lives, say a dozen experts". NBC News. 3 April 2020. https://www.nbcnews.com/politics/donald-trump/trump-administration-s-lack-unified-coronavirus-strategy-will-cost-lives-n1175126

34 Rojas, C.R., Richards, C. and Rhodes, C. 2021. Pathways to Linking Science and Policy in the Field of Global Risk. Centre for the Study of Existential Risk. University of Cambridge. 23 April 2021. https://www.cser.ac.uk/news/new-report-pathways-linking-science-and-policy-fie/

Appendices

GETTY/TIMANDTIM

APPENDIX A

Descriptions of Global Risks 2022

Global Risks

A "global risk" is the possibility of the occurrence of an event or condition that, if it occurs, could cause significant negative impact for several countries or industries. For the purposes of this report, the scope is over the next 10 years.

To ensure legibility, the names of the global risks have been abbreviated in the figures. The portion of the full name used in the abbreviation is in bold.

	Global Risk	Description
Economic	**Asset bubble bursts** in large economies	Prices for housing, investment funds, shares and other assets in a large economy increasingly disconnect from the real economy
	Collapse of a systemically important **industry**	Collapse of a systemically important global industry or firm with an impact on the global economy, financial markets and/or society
	Debt crises in large economies	Corporate and/or public finances overwhelmed by debt accumulation and/or debt servicing in large economies, resulting in mass bankruptcies, defaults, insolvency, liquidity crises or sovereign debt crises
	Failure to **stabilize price** trajectories	Inability to control an unmanageable increase (inflation) or decrease (deflation) in the general price level of goods and services
	Proliferation of **illicit economic activity**	Global proliferation of informal and/or illegal activities that undermine economic advancement and growth: counterfeiting, illicit financial flows, illicit trade, tax evasion, human trafficking, organized crime etc.
	Prolonged economic **stagnation**	Near-zero or slow global growth lasting for many years
	Severe **commodity shocks**	Abrupt shocks to the supply and demand of systemically important commodities at a global scale that strain corporate, public and/or household budgets: chemicals, emissions, energy, foods, metals, minerals etc.
Environmental	**Biodiversity loss** and ecosystem collapse	Irreversible consequences for the environment, humankind, and economic activity, and a permanent destruction of natural capital, as a result of species extinction and/ or reduction
	Climate action failure	Failure of governments and businesses to enforce, enact or invest in effective climate-change adaptation and mitigation measures, preserve ecosystems, protect populations and transition to a carbon-neutral economy
	Extreme weather events	Loss of human life, damage to ecosystems, destruction of property and/or financial loss at a global scale as a result of extreme weather events: cold fronts, fires, floods, heat waves, windstorms etc.
	Human-made **environmental damage**	Loss of human life, financial loss and/or damage to ecosystems as a result of human activity and/or failure to co-exist with animal ecosystems: deregulation of protected areas, industrial accidents, oil spills, radioactive contamination, wildlife trade etc.
	Major **geophysical disasters**	Loss of human life, financial loss and/or damage to ecosystems as a result of geophysical disasters: earthquakes, landslides, geomagnetic storms, tsunamis, volcanic activity etc.
	Natural resource crises	Chemical, food, mineral, water or other natural resource crises at a global scale as a result of human overexploitation and/or mismanagement of critical natural resources

Geopolitical	**Collapse** of a **multilateral** institution	Dissolution of a global multilateral institution established to resolve economic, environmental, geopolitical and/or humanitarian crises with regional or global implications: border disputes, environmental commitments, migration crises, health emergencies, trade disputes etc.
	Fracture of **interstate relations**	Economic, political and/or technological rivalries between geopolitical powers resulting in a fracture of bilateral relations and/or growing tensions
	Geoeconomic confrontations	Deployment of economic levers, including investment controls, trade controls, non-tariff barriers and/or currency measures, by global or regional powers to decouple economic interactions between nations and consolidate spheres of influence
	Geopolitical contestation of strategic **resources**	Concentration, exploitation and/or mobility restriction by a state of goods, knowledge, services or technology critical to human development with the intent of gaining geopolitical advantage
	Interstate conflict	Belligerent bilateral or multilateral conflict between states with global consequences: biological, chemical, cyber and/or physical attacks, military interventions, proxy wars etc.
	State collapse	Collapse of a state with global geopolitical importance as a result of internal conflict, breakdown of rule of law, erosion of institutions, military coup, regional or global instability
	Terrorist attacks	Large-scale, scattered or isolated terrorist attacks carried out by individuals or non-state groups with ideological, political or religious goals, resulting in loss of life, severe injury and/or material damage
	Weapons of mass destruction	Deployment of biological, chemical, cyber, nuclear or radiological weapons, resulting in loss of life, destruction and/or international crises
Societal	**Collapse** or lack of **social security** systems	Non-existence or widespread bankruptcy of social security systems and/or erosion of social security benefits: disability, elderly, family, injury, maternity, medical care, sickness, survivor, unemployment etc.
	Employment and **livelihood crises**	Structural deterioration of work prospects and/or standards for the working-age population: unemployment, underemployment, lower wages, fragile contracts, erosion of worker rights etc.
	Erosion of **social cohesion**	Loss of social capital and a fracture of social networks negatively impacting social stability, individual well-being and economic productivity as a result of persistent public anger, distrust, divisiveness, lack of empathy, marginalization of minorities, political polarization etc.
	Failure of **public infrastructure**	Unequitable and/or insufficient public infrastructure and services as a result of mismanaged urban sprawl, poor planning and/or under-investment, negatively impacting economic advancement, education, housing, public health, social inclusion and the environment
	Infectious diseases	Massive and rapid spread of viruses, parasites, fungi or bacteria that cause an uncontrolled contagion of infectious diseases, resulting in an epidemic or pandemic with loss of life and economic disruption
	Large-scale **involuntary migration**	Large-scale involuntary migration induced by climate change, discrimination, lack of economic advancement opportunities, persecution, natural or human-made disasters, violent conflict etc.
	Pervasive **backlash against science**	Censure, denial and/or scepticism towards scientific evidence and the scientific community at a global scale, resulting in a regression or stalling of progress on climate action, human health and/or technological innovation
	Pollution-driven **harms to human health**	Physical and mental health impacts from harmful chemical or other particulates in the air, water or food, which may stem from energy generation, industrial and agricultural practices, waste management failures, natural disasters, human behaviour and other sources
	Severe **mental health deterioration**	Pervasiveness of mental health ailments and/or disorders globally and across multiple demographics, negatively impacting well-being, social cohesion and productivity: anxiety, dementia, depression, loneliness, stress etc.
	Widespread **youth disillusionment**	Youth disengagement, lack of confidence and/or loss of trust of existing economic, political and social structures at a global scale, negatively impacting social stability, individual well-being and economic productivity

Technological	**Adverse** outcomes of **technological advances**	Intended or unintended negative consequences of technological advances on individuals, businesses, ecosystems and/or economies: AI, brain-computer interfaces, biotechnology, geo-engineering, quantum computing etc.
	Breakdown of critical information **infrastructure**	Deterioration, saturation or shutdown of critical physical and digital infrastructure or services as a result of a systemic dependency on cyber networks and/or technology: AI-intensive systems, internet, hand-held devices, public utilities, satellites etc.
	Digital inequality	Fractured and/or unequal access to critical digital networks and technology, between and within countries, as a result of unequal investment capabilities, lack of necessary skills in the workforce, insufficient purchase power, government restrictions and/or cultural differences
	Digital power concentration	Concentration of critical digital assets, capabilities and/or knowledge by a reduced number of individuals, businesses or states, resulting in discretionary pricing mechanisms, lack of impartial oversight, unequal private and/or public access etc.
	Failure of **cybersecurity** measures	Business, government and household cybersecurity infrastructure and/or measures are outstripped or rendered obsolete by increasingly sophisticated and frequent cybercrimes, resulting in economic disruption, financial loss, geopolitical tensions and/or social instability
	Failure of **technology governance**	Lack of globally accepted frameworks, institutions or regulations for the use of critical digital networks and technology, as a result of different states or groups of states adopting incompatible digital infrastructure, protocols and/or standards

APPENDIX B

Executive Opinion Survey: National Risk Perceptions

Table B.1 presents the top five risks for each of the 124 economies surveyed by the World Economic Forum's Executive Opinion Survey (EOS) between May and September 2021. Over 12,000 leaders answered the following question: "What five risks will pose a critical threat to your country in the next two years?" and were asked to select these from a list of 35 risks, with no particular order. "Risk 1" indicates the most frequently selected risk in each economy. Where there is a tie, the tied risks are presented alphabetically in the same cell, separated by a dotted line ("---") and the next cell in the row contains an ellipsis ("…"). For example, in Armenia, two risks ("human-made environmental damage" and "large-scale involuntary migration") are tied for third place and there is therefore no risk in fourth place.

The question posed to EOS respondents is comparable to the following question asked to GRPS respondents: "Please identify your top five global risks of concern [that will become a critical threat to the world] over the next 0–2 years". The list of 35 risks to select from in the EOS is also comparable to the list of risks in the Global Risks Perception Survey (GRPS), except for two new risks that were added to the GRPS after the EOS was conducted—"geoeconomic confrontations" and "pollution-driven harms to human health"—and one risk that changed name from "geopolitization of strategic resources" in the EOS to "geopolitical contestation of strategic resources" in the GRPS (see Appendix C, Global Risks Perception Survey Technical Notes).

TABLE B.1

Top Five Risks Identified by the Executive Opinion Survey

Economy	Risk 1	Risk 2	Risk 3	Risk 4	Risk 5
Albania	Fracture of interstate relations	Human-made environmental damage	Failure of cybersecurity measures	Debt crises in large economies	Infectious diseases
Angola	Employment and livelihood crises	Prolonged economic stagnation	Human-made environmental damage	State collapse	Widespread youth disillusionment
Argentina	Prolonged economic stagnation	Employment and livelihood crises	State collapse	Failure to stabilize price trajectories	Digital inequality
Armenia	Interstate conflict	Prolonged economic stagnation	Human-made environmental damage --- Large-scale involuntary migration	…	Failure of cybersecurity measures --- Fracture of interstate relations
Australia	Failure of cybersecurity measures	Extreme weather events	Climate action failure	Infectious diseases	Debt crises in large economies

Economy	Risk 1	Risk 2	Risk 3	Risk 4	Risk 5
Austria	Climate action failure	Erosion of social cohesion	Debt crises in large economies	Digital power concentration	Prolonged economic stagnation Extreme weather events
Azerbaijan	Natural resource crises	Asset bubble bursts in large economies	Debt crises in large economies	Climate action failure Collapse of a multilateral institution Human-made environmental damage Infectious diseases	…
Bahrain	Prolonged economic stagnation	Debt crises in large economies Failure of cybersecurity measures	…	Infectious diseases	Employment and livelihood crises
Bangladesh	Employment and livelihood crises	Digital inequality Geopolitization of strategic resources	…	Human-made environmental damage	Climate action failure Failure of cybersecurity measures
Barbados	Extreme weather events	Prolonged economic stagnation	Employment and livelihood crises	Collapse of a systemically important industry	Climate action failure Infectious diseases
Belgium	Climate action failure	Debt crises in large economies	Extreme weather events	Asset bubble bursts in large economies Fracture of interstate relations	…
Benin	Proliferation of illicit economic activity	Failure to stabilize price trajectories	Severe commodity shocks	Pervasive backlash against science	Erosion of social cohesion
Bolivia	Employment and livelihood crises	Proliferation of illicit economic activity	Digital inequality Human-made environmental damage	…	State collapse

Economy	Risk 1	Risk 2	Risk 3	Risk 4	Risk 5
Bosnia and Herzegovina	Human-made environmental damage Prolonged economic stagnation	…	Employment and livelihood crises	Digital inequality Widespread youth disillusionment	…
Botswana	Employment and livelihood crises	Collapse or lack of social security systems	Prolonged economic stagnation	Widespread youth disillusionment	Debt crises in large economies
Brazil	Prolonged economic stagnation	Employment and livelihood crises	Digital inequality	Human-made environmental damage	Geopolitization of strategic resources
Brunei Darussalam	Employment and livelihood crises	Prolonged economic stagnation	Failure of technology governance	Human-made environmental damage	Failure of cybersecurity measures
Bulgaria	Human-made environmental damage	Infectious diseases	Interstate conflict	Debt crises in large economies Employment and livelihood crises	…
Cambodia	Human-made environmental damage	Prolonged economic stagnation	Adverse outcomes of technological advances Infectious diseases	…	Biodiversity loss and ecosystem collapse Debt crises in large economies
Cameroon	Employment and livelihood crises	Terrorist attacks	Debt crises in large economies	Human-made environmental damage	Natural resource crises
Canada	Debt crises in large economies	Climate action failure	Extreme weather events	Employment and livelihood crises	Infectious diseases
Cape Verde	Employment and livelihood crises	Prolonged economic stagnation	Human-made environmental damage	Debt crises in large economies	Biodiversity loss and ecosystem collapse Failure of cybersecurity measures
Chad	Debt crises in large economies	Employment and livelihood crises	Breakdown of critical information infrastructure	Terrorist attacks	Human-made environmental damage
Chile	Prolonged economic stagnation	Erosion of social cohesion	Collapse or lack of social security systems	State collapse	Extreme weather events

Economy	Risk 1	Risk 2	Risk 3	Risk 4	Risk 5
China	Extreme weather events	Asset bubble bursts in large economies	Infectious diseases	Collapse or lack of social security systems	Geopolitization of strategic resources
Colombia	Employment and livelihood crises	Human-made environmental damage	Prolonged economic stagnation	State collapse	Proliferation of illicit economic activity
Congo	Employment and livelihood crises Human-made environmental damage	…	Biodiversity loss and ecosystem collapse Digital inequality	…	Interstate conflict State collapse
Costa Rica	Prolonged economic stagnation	Employment and livelihood crises	Digital inequality	State collapse	Debt crises in large economies Extreme weather events
Côte d'Ivoire	Terrorist attacks	Debt crises in large economies	Failure to stabilize price trajectories	Employment and livelihood crises	Human-made environmental damage
Croatia	Prolonged economic stagnation	Geopolitization of strategic resources	Digital inequality	Human-made environmental damage	Widespread youth disillusionment
Cyprus	Climate action failure	Debt crises in large economies	Geopolitization of strategic resources	Asset bubble bursts in large economies Infectious diseases Prolonged economic stagnation	…
Czech Republic	Debt crises in large economies	Collapse of a systemically important industry	Asset bubble bursts in large economies	Infectious diseases	Failure to stabilize price trajectories
Denmark	Climate action failure	Asset bubble bursts in large economies Infectious diseases	…	Failure of cybersecurity measures	Debt crises in large economies
Dominican Republic	Extreme weather events	Employment and livelihood crises	Debt crises in large economies	Digital inequality Failure of cybersecurity measures	…

Economy	Risk 1	Risk 2	Risk 3	Risk 4	Risk 5
Ecuador	Collapse or lack of social security systems	Prolonged economic stagnation	Employment and livelihood crises	Proliferation of illicit economic activity	Digital inequality
Egypt	Natural resource crises	Infectious diseases	Debt crises in large economies	Failure to stabilize price trajectories	Employment and livelihood crises
El Salvador	Prolonged economic stagnation	State collapse	Extreme weather events	Employment and livelihood crises	Collapse or lack of social security systems Digital inequality
Estonia	Interstate conflict	Debt crises in large economies	Asset bubble bursts in large economies Fracture of interstate relations	…	Human-made environmental damage
Finland	Prolonged economic stagnation	Debt crises in large economies	Climate action failure	Asset bubble bursts in large economies	Infectious diseases
France	Erosion of social cohesion	Debt crises in large economies Geopolitization of strategic resources	…	Climate action failure	Failure of cybersecurity measures
Georgia	Interstate conflict	Digital inequality	Failure to stabilize price trajectories	Debt crises in large economies	Employment and livelihood crises
Germany	Climate action failure	Erosion of social cohesion	Digital power concentration	Debt crises in large economies	Fracture of interstate relations Geopolitization of strategic resources
Ghana	Employment and livelihood crises Human-made environmental damage	…	Geopolitization of strategic resources	Failure of cybersecurity measures	Collapse of a systemically important industry
Greece	Prolonged economic stagnation	Extreme weather events	Debt crises in large economies	Interstate conflict	Digital inequality

Economy	Risk 1	Risk 2	Risk 3	Risk 4	Risk 5
Guatemala	Proliferation of illicit economic activity	State collapse	Extreme weather events	Failure of public infrastructure	Erosion of social cohesion Human-made environmental damage
Honduras	State collapse	Employment and livelihood crises	Extreme weather events	Proliferation of illicit economic activity	Prolonged economic stagnation
Hong Kong SAR, China	Asset bubble bursts in large economies	Prolonged economic stagnation	Infectious diseases	Interstate conflict	Erosion of social cohesion
Hungary	Failure to stabilize price trajectories	Extreme weather events	Climate action failure	Infectious diseases	Fracture of interstate relations
Iceland	Asset bubble bursts in large economies Climate action failure	…	Collapse of a systemically important industry	Failure of cybersecurity measures Infectious diseases	…
India	Fracture of interstate relations	Debt crises in large economies	Widespread youth disillusionment	Failure of technology governance	Digital inequality
Indonesia	Debt crises in large economies Human-made environmental damage	…	Employment and livelihood crises	Geopolitization of strategic resources	Failure of cybersecurity measures
Iran	Employment and livelihood crises	Widespread youth disillusionment	Prolonged economic stagnation	Natural resource crises	Biodiversity loss and ecosystem collapse
Ireland	Climate action failure Failure of cybersecurity measures	…	Fracture of interstate relations	Debt crises in large economies Prolonged economic stagnation	…
Israel	Terrorist attacks	Asset bubble bursts in large economies Interstate conflict	…	Failure of cybersecurity measures	Weapons of mass destruction
Italy	Climate action failure Debt crises in large economies	…	Extreme weather events	Geopolitization of strategic resources	Digital inequality

Economy	Risk 1	Risk 2	Risk 3	Risk 4	Risk 5
Japan	Prolonged economic stagnation	Extreme weather events	Interstate conflict	Failure of cybersecurity measures	Asset bubble bursts in large economies Infectious diseases
Jordan	Debt crises in large economies	Employment and livelihood crises	Natural resource crises	Prolonged economic stagnation	Failure to stabilize price trajectories
Kazakhstan	Employment and livelihood crises Failure to stabilize price trajectories	…	Severe commodity shocks	Interstate conflict	Geopolitization of strategic resources
Kenya	Employment and livelihood crises	Debt crises in large economies	Human-made environmental damage	Prolonged economic stagnation Terrorist attacks	…
Republic of Korea	Asset bubble bursts in large economies	Employment and livelihood crises Infectious diseases	…	Debt crises in large economies	Human-made environmental damage
Kuwait	Asset bubble bursts in large economies Collapse or lack of social security systems	…	Failure of technology governance Geopolitization of strategic resources	…	Human-made environmental damage Infectious diseases
Kyrgyzstan	Employment and livelihood crises	Interstate conflict	Failure of technology governance	Climate action failure	Failure to stabilize price trajectories
Lao PDR	Failure to stabilize price trajectories	Employment and livelihood crises	Human-made environmental damage	Biodiversity loss and ecosystem collapse	Breakdown of critical information infrastructure Infectious diseases
Latvia	Interstate conflict	Asset bubble bursts in large economies	Digital inequality	Debt crises in large economies Prolonged economic stagnation	…

Economy	Risk 1	Risk 2	Risk 3	Risk 4	Risk 5
Lebanon	State collapse	Human-made environmental damage	Collapse or lack of social security systems	Debt crises in large economies Prolonged economic stagnation	…
Lesotho	Digital inequality	Infectious diseases	Climate action failure	Extreme weather events	Debt crises in large economies
Lithuania	Interstate conflict	Severe commodity shocks	Asset bubble bursts in large economies Failure of cybersecurity measures	…	Human-made environmental damage
Luxembourg	Asset bubble bursts in large economies	Climate action failure Debt crises in large economies	…	Digital inequality Fracture of interstate relations	…
Malawi	Failure to stabilize price trajectories	Human-made environmental damage Prolonged economic stagnation	…	Proliferation of illicit economic activity	Debt crises in large economies Employment and livelihood crises
Malaysia	Human-made environmental damage	Employment and livelihood crises	Prolonged economic stagnation	Geopolitization of strategic resources	Debt crises in large economies
Mali	Employment and livelihood crises Terrorist attacks	…	Debt crises in large economies	Collapse or lack of social security systems	Failure of technology governance
Malta	Human-made environmental damage	Collapse of a systemically important industry	Proliferation of illicit economic activity	Failure of cybersecurity measures	Asset bubble bursts in large economies
Mauritius	Prolonged economic stagnation	Collapse of a systemically important industry	Employment and livelihood crises	Extreme weather events	Erosion of social cohesion
Mexico	Proliferation of illicit economic activity	Prolonged economic stagnation	State collapse	Employment and livelihood crises	Digital inequality
Moldova	Prolonged economic stagnation	Large-scale involuntary migration	Interstate conflict	Extreme weather events	Proliferation of illicit economic activity

Economy	Risk 1	Risk 2	Risk 3	Risk 4	Risk 5
Mongolia	Human-made environmental damage	Employment and livelihood crises	Prolonged economic stagnation State collapse	…	Geopolitization of strategic resources
Montenegro	Employment and livelihood crises	Fracture of interstate relations	Prolonged economic stagnation	Digital inequality	Human-made environmental damage
Morocco	Natural resource crises	Employment and livelihood crises	Prolonged economic stagnation	Digital inequality	Extreme weather events Interstate conflict
Namibia	Employment and livelihood crises	Digital inequality	Prolonged economic stagnation	Extreme weather events	Debt crises in large economies
Nepal	Employment and livelihood crises	Human-made environmental damage	Geopolitization of strategic resources	Infectious diseases	Digital inequality Prolonged economic stagnation
Netherlands	Climate action failure	Erosion of social cohesion	Failure of cybersecurity measures	Asset bubble bursts in large economies	Debt crises in large economies
New Zealand	Failure of cybersecurity measures	Asset bubble bursts in large economies Infectious diseases Prolonged economic stagnation	…	…	Climate action failure Extreme weather events
Nicaragua	State collapse	Prolonged economic stagnation	Employment and livelihood crises Extreme weather events	…	Collapse or lack of social security systems
Nigeria	Terrorist attacks	Prolonged economic stagnation	Widespread youth disillusionment	Employment and livelihood crises	Human-made environmental damage
North Macedonia	Human-made environmental damage	Failure of public infrastructure	Debt crises in large economies	Prolonged economic stagnation	Digital inequality
Pakistan	Debt crises in large economies	Extreme weather events	Failure to stabilize price trajectories	Failure of cybersecurity measures	Human-made environmental damage

Economy	Risk 1	Risk 2	Risk 3	Risk 4	Risk 5
Panama	Collapse or lack of social security systems	Prolonged economic stagnation	Employment and livelihood crises	Digital inequality	Human-made environmental damage
Paraguay	Proliferation of illicit economic activity	Collapse or lack of social security systems	Digital inequality	Human-made environmental damage	Employment and livelihood crises State collapse
Peru	State collapse	Prolonged economic stagnation	Employment and livelihood crises	Digital inequality	Human-made environmental damage Proliferation of illicit economic activity
Philippines	Prolonged economic stagnation	Digital inequality	Extreme weather events	Employment and livelihood crises	Failure of public infrastructure
Poland	Human-made environmental damage	Infectious diseases	Interstate conflict	Fracture of interstate relations Prolonged economic stagnation	…
Portugal	Prolonged economic stagnation	Debt crises in large economies	Employment and livelihood crises	Digital inequality	Collapse or lack of social security systems
Qatar	Climate action failure	Digital inequality	Collapse of a systemically important industry Fracture of interstate relations Infectious diseases Natural resource crises	…	…
Romania	Human-made environmental damage	Employment and livelihood crises	Debt crises in large economies Geopolitization of strategic resources	…	Large-scale involuntary migration
Russian Federation	Interstate conflict	Failure to stabilize price trajectories	Infectious diseases	Employment and livelihood crises	Severe commodity shocks

Economy	Risk 1	Risk 2	Risk 3	Risk 4	Risk 5
Rwanda	Employment and livelihood crises	Prolonged economic stagnation	Extreme weather events	Digital inequality	Failure of cybersecurity measures
Saudi Arabia	Failure to stabilize price trajectories	Human-made environmental damage Infectious diseases	…	Interstate conflict	Fracture of interstate relations Prolonged economic stagnation
Senegal	Employment and livelihood crises	Debt crises in large economies	Terrorist attacks	Human-made environmental damage	Digital inequality Natural resource crises
Serbia	Human-made environmental damage	Debt crises in large economies	Employment and livelihood crises	Digital inequality	Geopolitization of strategic resources
Sierra Leone	Employment and livelihood crises	Human-made environmental damage	Prolonged economic stagnation	Failure to stabilize price trajectories	Widespread youth disillusionment
Singapore	Prolonged economic stagnation	Infectious diseases	Asset bubble bursts in large economies	Failure of cybersecurity measures	Climate action failure
Slovakia	Collapse of a systemically important industry	Collapse or lack of social security systems	Debt crises in large economies Human-made environmental damage	…	Digital inequality
Slovenia	Severe commodity shocks	Geopolitization of strategic resources	Asset bubble bursts in large economies	Extreme weather events Human-made environmental damage	…
South Africa	Prolonged economic stagnation	Employment and livelihood crises	State collapse	Failure of public infrastructure	Proliferation of illicit economic activity
Spain	Employment and livelihood crises	Prolonged economic stagnation	Debt crises in large economies	Climate action failure Fracture of interstate relations	…

Economy	Risk 1	Risk 2	Risk 3	Risk 4	Risk 5
Sri Lanka	Human-made environmental damage	Debt crises in large economies	Employment and livelihood crises Infectious diseases	…	Digital inequality
Sweden	Asset bubble bursts in large economies	Terrorist attacks	Climate action failure	Debt crises in large economies	Human-made environmental damage
Switzerland	Asset bubble bursts in large economies	Prolonged economic stagnation	Debt crises in large economies Fracture of interstate relations Geopolitization of strategic resources Interstate conflict	…	…
Taiwan, China	Infectious diseases	Extreme weather events	Geopolitization of strategic resources	Failure of cybersecurity measures	Asset bubble bursts in large economies
Tajikistan	Interstate conflict	Failure to stabilize price trajectories	Extreme weather events	Employment and livelihood crises Infectious diseases	…
Tanzania	Debt crises in large economies	Employment and livelihood crises	Human-made environmental damage	Climate action failure Infectious diseases	…
Thailand	Debt crises in large economies	Human-made environmental damage	Prolonged economic stagnation	Digital inequality	Employment and livelihood crises
Trinidad and Tobago	Prolonged economic stagnation	Employment and livelihood crises	Digital inequality	Collapse of a systemically important industry	Extreme weather events
Tunisia	State collapse	Debt crises in large economies	Employment and livelihood crises	Prolonged economic stagnation	Proliferation of illicit economic activity
Turkey	Employment and livelihood crises	Prolonged economic stagnation	Fracture of interstate relations	Human-made environmental damage	Failure of technology governance

Economy	Risk 1	Risk 2	Risk 3	Risk 4	Risk 5
Ukraine	Prolonged economic stagnation	State collapse	Climate action failure Failure to stabilize price trajectories Interstate conflict	…	…
United Arab Emirates	Infectious diseases	Asset bubble bursts in large economies	Debt crises in large economies Failure of cybersecurity measures	…	Climate action failure Employment and livelihood crises
United Kingdom	Failure of cybersecurity measures	Debt crises in large economies	Prolonged economic stagnation	Infectious diseases	Extreme weather events
United States	Asset bubble bursts in large economies	Climate action failure	Extreme weather events	Debt crises in large economies	Employment and livelihood crises
Uruguay	Severe commodity shocks	Prolonged economic stagnation	Employment and livelihood crises	Extreme weather events	Collapse or lack of social security systems
Venezuela	State collapse	Prolonged economic stagnation	Human-made environmental damage	Large-scale involuntary migration	Proliferation of illicit economic activity
Viet Nam	Biodiversity loss and ecosystem collapse	Asset bubble bursts in large economies	Infectious diseases	Extreme weather events Geopolitization of strategic resources	…
Yemen	Failure to stabilize price trajectories	State collapse	Failure of public infrastructure	Employment and livelihood crises Interstate conflict Natural resource crises	…
Zambia	Employment and livelihood crises	Debt crises in large economies	Failure to stabilize price trajectories	Human-made environmental damage	Prolonged economic stagnation

APPENDIX C

Technical Notes: Global Risks Perception Survey 2021–2022

The Global Risks Perception Survey (GRPS) is the World Economic Forum's source of original risks data, harnessing the expertise of the Forum's extensive network of academic, business, government, civil society and thought leaders. Survey responses were collected from 8 September to 12 October 2021 from the World Economic Forum's multistakeholder communities (including the Global Shapers Community), the professional networks of its Advisory Board, and members of the Institute of Risk Management. The results of the GRPS are used to create the graphics depicting the Global Risks COVID-19 Hindsight, Future Outlook, the Global Risks Horizon, Global Risks Severity, Global Risks Effects and International Risk Mitigation Efforts presented at the beginning of the report and to offer insights used throughout.

Both the GRPS and the *Global Risks Report* adopt the following definition: *a global risk is the possibility of the occurrence of an event or condition which, if it occurs, could cause significant negative impact for several countries or industries. For the purposes of this report, the scope is over the next 10 years.*

Updates in the GRPS 2021–2022

New list of risks

The list of 37 global risks included in the survey was updated in 2021.

Two new risks were added in response to observed economic, geopolitical and environmental trends. These new risks are: (1) "Geoeconomic confrontations" and (2) "Pollution harms to human health".

The names and definitions of the remaining 35 risks have been revised and, where applicable, have been modified and/or expanded to reflect new ways in which the risks may materialize and the potential adverse outcomes they may cause. However, to ensure comparability over time, although names and definitions were modified, the fundamental concept of the risk remained consistent with that in previous versions of the survey.

New sections

The GRPS 2021–2022 was extensively reformed this year to gather fresher, broader and more informed risk perceptions and to incorporate new approaches to risk management and analysis. The GRPS 2021–2022 is comprised of six sections:

1. **COVID-19 Hindsight and Future Outlook (new):** asks respondents to form an opinion about how the COVID-19 pandemic aggravated risks, permitting some comparability with GRPS results from previous years. This opinion then facilitates the projection of their views forward beyond the pandemic. This section also captures respondent sentiment on the outlook for the world to inform an analysis of how individual contexts may influence global risk perceptions and the perceived status of mitigation efforts.

2. **Global Risks Horizon**: recognizes that respondents may have varying perceptions on the evolution of global risks within a 10-year horizon. This section asks respondents to take a view on risks in the short term (0–2 years), medium term (2–5 years) and long term (5–10 years), also capturing respondents' sense of urgency about global risks and informing an analysis of choices and trade-offs that may face decision-makers.

3. **Global Risks Severity (new):** asks respondents to rank the potential damage of a global risk over the next 10 years and reminds respondents to consider multiple criteria—including human suffering, societal disruption, economic shock, environmental degradation and political instability. This section

uses ranking rather than a 1–5 rating scale to allow respondents to answer the question with more confidence.

4. **Global Risks Effects (new):** recognizing that risks are not isolated but affect and amplify each other through negative feedback loops, this section incentivizes a holistic view of global risks by asking respondents to consider cascading impacts in conjunction with the severity of the risk itself.

5. **Global Governance – International Risk Mitigation Efforts (new):** recognizing that risk mitigation needs to be a part of the global agenda, this section asks respondents to assess the current state of international mitigation efforts in 15 global governance areas. It identifies achievements and areas of opportunity for global action and cooperation and informs an analysis of how the various stages of effectiveness may influence future preparedness.

6. **Open Questions (new):** complements risk identification with a series of questions to detect blind spots, trends and shocks. This section ensures that the GRPS is a flexible and engaging mechanism to source expert knowledge.

Methodology

COVID-19 Hindsight & Future Outlook

COVID-19 Hindsight:
For each of the 37 global risks listed in Appendix A, respondents were asked to identify three global risks that they believe had worsened since the start of the COVID-19 crisis. A simple tally for each of the 37 global risks was calculated on this basis. The results are illustrated in Figure I.

Future Outlook:
Respondents were asked to express their feeling about the outlook for the world in four sentiments: worried, concerned, positive, optimistic. A simple tally for each of the four sentiments was calculated on this basis. The results are illustrated in Figure 1.2.

Respondents were then asked to characterize their outlook for the world over the next 3 years with the following four answer options: accelerating global recovery; fractured trajectories, separating winners and losers; consistently volatile with multiple surprises; progressive tipping points with increasing catastrophic outcomes. A simple tally for each of the four sentiments was calculated on this basis. The results are illustrated in Figure 1.1.

Global Risks Horizon

For each of the 37 global risks listed in Appendix A, respondents were asked to identify when they believe a risk will become a critical threat to the world, within the following timeframes:

- Short-term threats: 0–2 years
- Medium-term threats: 2–5 years
- Long-term threats: 5–10 years

A simple tally for each of the 37 global risks was calculated on this basis. the results are illustrated in Figure II.

Global Risks Severity

For each of the 37 global risks listed in Appendix A, respondents were asked to choose nine risks and rank order them from 1 to 9 according to their perceived severity of impact—"most severe" was defined as having the potential to yield the most damage on a global scale within the next 10 years. Respondents were asked to value the impact of risks considering multiple criteria, including human suffering, societal disruption, economic shock, environmental degradation and political instability.

The results were aggregated according to the following scoring schedule:

- 9 points each time a risk was selected as the most severe risk
- 8 points each time a risk was selected as the second-most severe risk
- 7 points each time a risk was selected as the third-most severe risk
- 6 points each time a risk was selected as the fourth-most severe risk

- 5 points each time a risk was selected as the fifth-most severe risk
- 4 points each time a risk was selected as the sixth-most severe risk
- 3 points each time a risk was selected as seventh-most severe risk
- 2 points each time a risk was selected as the eighth-most severe risk
- 1 point each time a risk was selected as the ninth-most severe risk

A simple sum of the scores for each of the risks according to the above scoring schedule was calculated on this basis. The results are illustrated in Figure 1.3.

Global Risks Effects

In the Global Risks Severity component, for each of the risks ranked most severe, second-most severe and third-most severe, respondents were then asked to select two risks that will be aggravated by those top severe risks.

A simple tally of the number of times a risk was identified as being aggravated by another for each of the most, second-, third-, fourth- and fifth-most severe risks was calculated on this basis. The results are illustrated in the Global Risks Effects (Figure III).

In the Global Risks Effects graph, the size of each of the most concerning risk nodes is scaled according to the above scoring schedule. The thickness of each of the links between a risk and the risks being aggravated is scaled according to the above tally.

Global Governance – International Risk Mitigation Efforts

From 15 international risk areas listed below, respondents were asked to rate the state each area was with regard to international risk mitigation efforts: "not started", "early development", "established", or "effective".

A simple tally for each of the four possible states was calculated on this basis. The results are illustrated in Figure IV.

The 15 international areas were: Artificial Intelligence (e.g., autonomous weapons, bias); Basic resource security (food and water); Biodiversity preservation; Climate change mitigation; Cross-border cyberattacks and misinformation; Financial system stability; Human health crises; International crime; Migration and refugees; Natural disaster relief; Physical conflict resolution; Poverty alleviation; Space exploitation; Trade facilitation; Weapons of mass destruction.

Completion thresholds

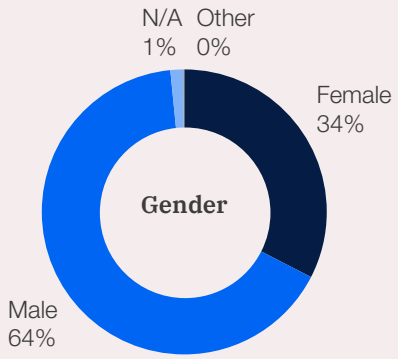
A total of 1,183 responses to the GRPS were received. From these, 959 were kept, using as a threshold at least one non-demographic answer.

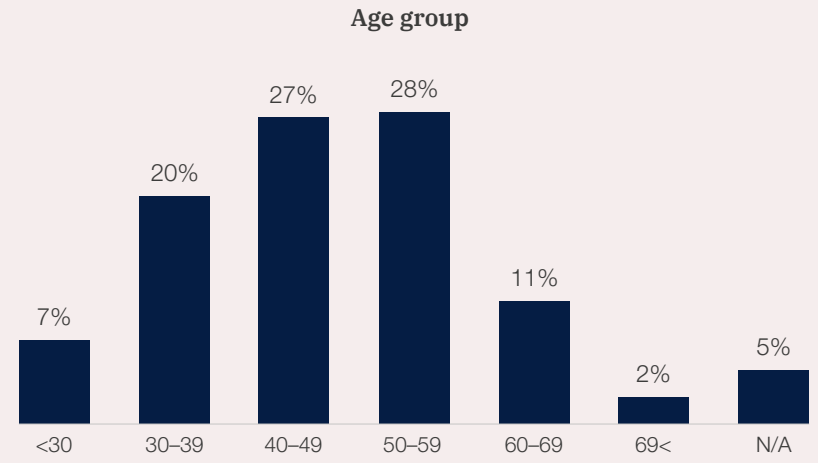
- **Section 1 - COVID-19 Hindsight & Future Outlook:** 959 respondents selected the three global risks.
  - **Future Sentiment:** 957
  - **Future Outlook:** 957
- **Section 2 - Global Risks Horizon:** 926 (0–2 years); 912 (2–5 years); 904 (5–10 years) respondents placed at least one risk within a possible timeframe. The results were computed among all respondents of the survey.
- **Section 3 - Global Risks Severity:** 893 respondents; 888 ranked at least one severe risk and assigned at least one driver.
- **Section 4 - Global Risks Effects:** 837 respondents identified at least one risk aggravating another.
- **Section 5 – Global Governance – International Risk Mitigation Efforts:** 829 (climate change) respondents scored at least one level of response, either global or regional. The results were computed among all respondents of each risk area within the section.
- **Sample distribution:** the 959 respondents from Section 1 were used to calculate the sample distribution by place of residence (region), gender, age, area of expertise and institution.

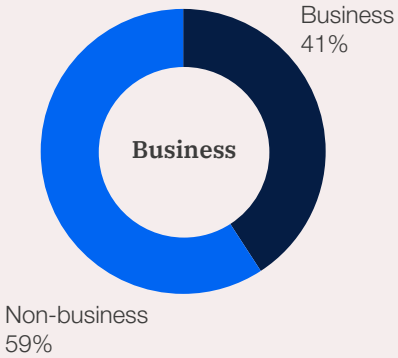
Figure C.1 presents some key descriptive statistics and information about the profiles of the respondents.

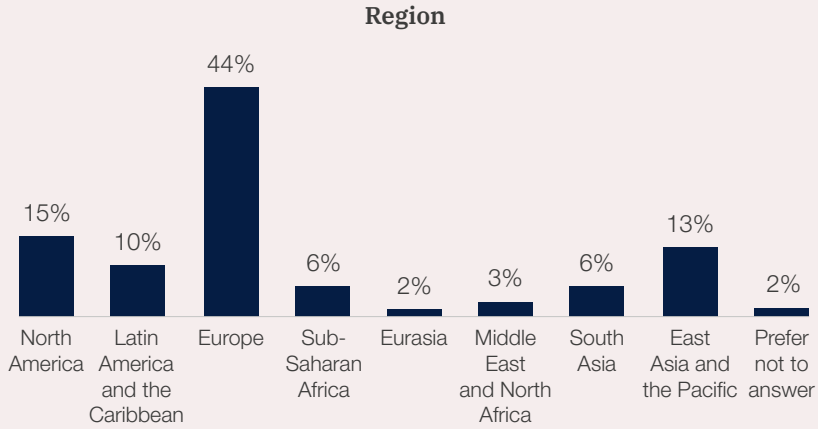
TABLE C.1

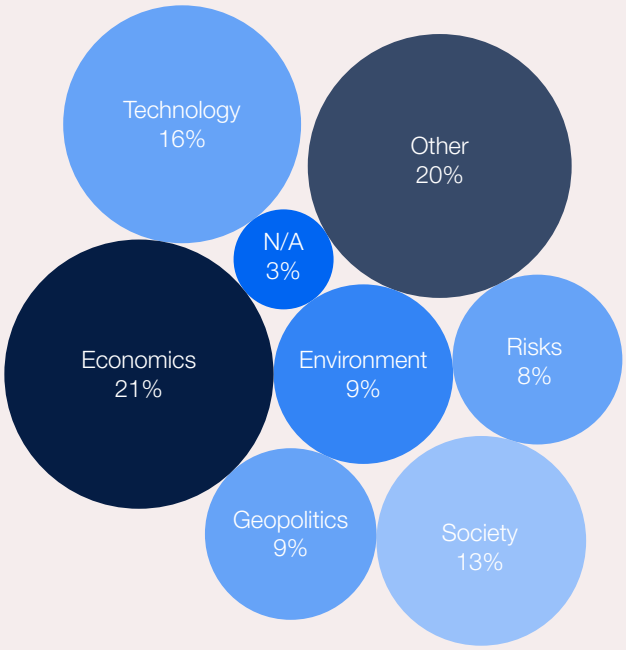
Survey Sample Composition

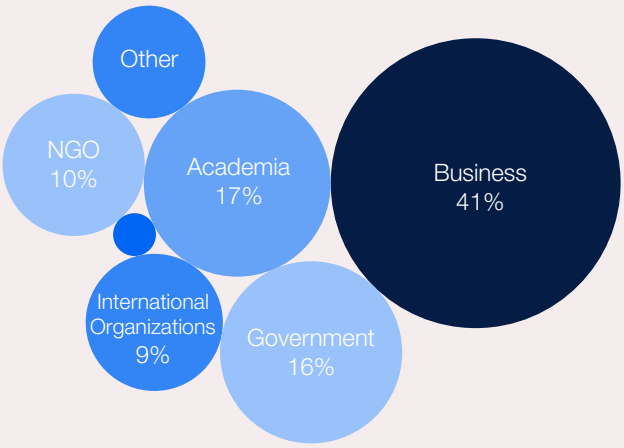




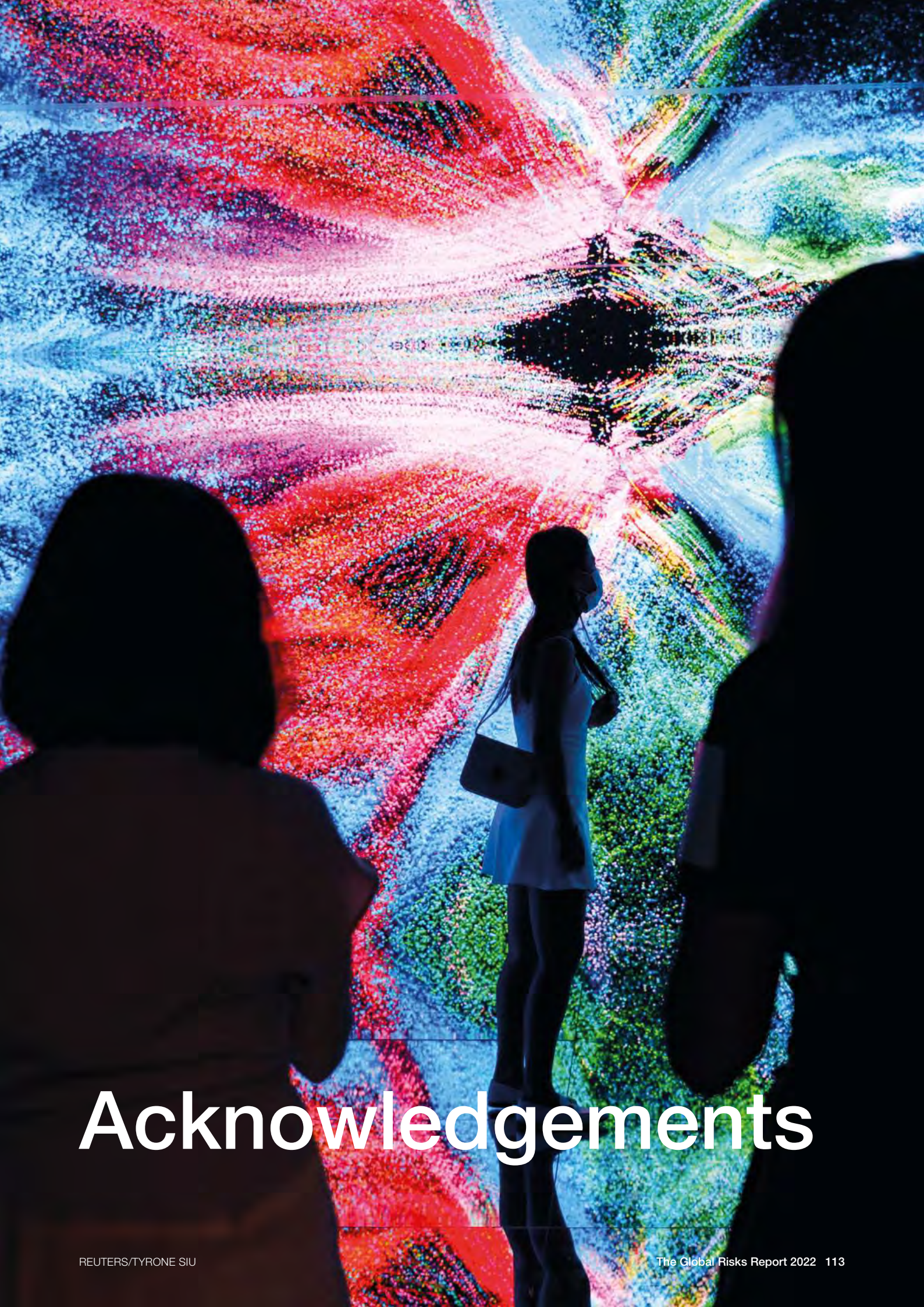








Source: World Economic Forum Global Risks Perception Survey 2021–2022



Acknowledgements

REUTERS/TYRONE SIU

Contributors

Emilio Granados Franco
Head of Global Risks and Geopolitical Agenda

Melinda Kuritzky
Lead, Global Risks and Geopolitical Agenda

Richard Lukacs
Specialist, Global Risks and Geopolitical Agenda

Saadia Zahidi
Managing Director, World Economic Forum

At the World Economic Forum, a debt of gratitude is owed to Professor Klaus Schwab (Founder and Executive Chairman) and Børge Brende (President), under whose guidance this report has been produced.

This report has relied heavily on the dedication and expertise of the World Economic Forum Platform for Shaping the Future of the New Economy and Society as well as other members of the *Global Risks Report 2022* team: Aidan Manktelow, Jordynn McKnight, Giovanni Salvi, Jean-Philippe Stanway, Samuel Werthmüller and Yann Zopf.

*****

We would like to thank our **Strategic Partners**, Marsh McLennan, SK Group, and Zurich Insurance Group, and particularly Daniel Glaser (President and Chief Executive Officer, Marsh McLennan), Chey Tae-won (Chairman and CEO, SK Group) and Mario Greco (Chief Executive Officer, Zurich Insurance Group). Thanks also to Carolina Klint (Managing Director, Risk Management Leader Continental Europe, Marsh), Lee Hyunghee (President, Social Value Committee, SK Group) and Peter Giger (Group Chief Risk Officer, Zurich Insurance Group).

Special gratitude is due to Guillaume Barthe-Dejean (Director, Chairman's Office, SK Group), John Scott (Head of Sustainability Risks, Zurich Insurance Group) and Richard Smith-Bingham (Executive Director, Marsh McLennan Advantage) for their contributions throughout the planning and drafting of the report.

We are also grateful to our three **Academic Advisers**: the National University of Singapore, the Oxford Martin School at the University of Oxford and the Wharton Risk Management and Decision Processes Center at the University of Pennsylvania.

The report has greatly benefited from the insight and expertise of the members of the *Global Risks Report* **Advisory Board**: Rolf Alter (Hertie School of Governance), Gabriella Bucher (Oxfam), Sharan Burrow (International Trade Union Confederation), Winnie Byanyima (UNAIDS), Marie-Valentine Florin (International Risk Governance Center), Charles Godfray (Oxford Martin School), Al Gore (Generation Investment Management), Lee Hyunghee (President, Social Value Committee, SK Group), Carolyn Kousky (Wharton Risk Management and Decision Processes Center), Pascal Lamy (Jacques Delors Institute), Robert Muggah (Igarapé Institute), Moisés Naím (Carnegie Endowment for International Peace), Carlos Afonso Nobre (University of São Paulo), Naomi Oreskes (Harvard University), Jonathan Ostry (International Monetary Fund), Carol Ouko-Misiko (Institute of Risk Management), Eduardo Pedrosa (Pacific Economic Cooperation Council), Danny Quah (National University of Singapore), Daniel Ralph (Cambridge Centre for Risk Studies), Samir Saran (Observer Research Foundation), John Scott (Zurich Insurance Group), Richard Smith-Bingham (Marsh McLennan), Effy Vayena (Swiss Federal Institute of Technology Zurich), Charlotte Warakaulle (CERN), Beatrice Weder di Mauro (Graduate Institute Geneva), Ngaire Woods (University of Oxford) and Alexandra Zapata (New America).

We would also like to thank SalesForce (Natalia Latimer, Vice President of Executive Engagement), Tableau (Neal Myrick, Vice President of Social Impact) and Lovelytics (Eric Balash) for the design of the interactive global risks data visualization.

*****

We are grateful to the following individuals from our Strategic Partners, Academic Advisers and Risk Communities.

Marsh McLennan: Rob Bailey, Amy Barnes, Francis Bouchard, Jerome Bouchard, Kate Bravery, Darrel Chang, Cheryl Cosslett, James Crask, Apoorv Dabral, Simon Glynn, Garrett Hanrahan, Ben Hoster, Rachel Juay, Stephen Kay, Christopher Labrecque, Siobhan O'Brien, Deepakshi Rawat, Jillian Reid, Claudio Saffioti, Reid Sawyer, Chris Smy, Sarah Stephens, Neil Frank Stevens and Scott Stransky.

Zurich Insurance Group: Paige Adams, Ines Bourbon, Laura Castellano, John Corless, Oliver Stephen Delvos, Daniel Eherer, Matt Holmes, Wen Lin, Sean McAllister,

Guy Miller, Eugenie Molyneux, Darren Nulty, Pavel Osipyants, Timothy Powell and Alessio Vinci.

SK Group: Ilbum Kim.

National University of Singapore: Tan Eng Chye and Ho Teck Hua.

Oxford Martin School: Julian Laird.

Wharton: Howard Kunreuther.

Global Future Council on Frontier Risks: Eric Parrado (Inter-American Development Bank, Council Co-Chair), Ngaire Woods (University of Oxford, Council Co-Chair), Clarissa Rios Rojas (University of Cambridge, Council Fellow), Deborah Ashby (Imperial College London), Elhadj As Sy (Kofi Annan Foundation), Nayef Al-Rodhan (University of Oxford), Guillaume Barthe-Dejean (SK Group), Nita A. Farahany (Duke University), Pascale Fung (Hong Kong University of Science and Technology), Alexander Gabuev (Carnegie Moscow Center), Florence Gaub (EU Institute for Security Studies), Sergei Guriev (Sciences Po), Orit Halpern (Concordia University), Maha Hosain Aziz (New York University), Meng Ke (Tsinghua University), Patricia Lerner (Greenpeace International), Liu Meng (UN Global Compact), Amrita Narlikar (German Institute for Global and Area Studies), Maria Soledad Nuñez Mendez (UCOM University), Jake Okechukwu Effoduh (Global Shaper), Peter Piot (London School of Hygiene and Tropical Medicine), John Scott (Zurich Insurance Group), Richard Smith-Bingham (Marsh McLennan), Tatiana Valovaya (United Nations Geneva), Gail Whiteman (Lancaster University Management School), Michele Wucker (Gray Rhino & Company) and Daria Zakharova (International Monetary Fund).

Chief Risk Officers Community: Stacy Allen (Lord Abbott), Bob Blakely (Team 8), Christian Bluhm (UBS AG), Brenda Boultwood (International Monetary Fund), Dzhangir Dzhangirov (Sberbank), Giancarlo Fancel (Generali), Sebastian Fritz-Morgenthal (Bain & Company Inc.), Peter Giger (Zurich Insurance Group), Jan Hansen (Novartis), Bahare Heywood (Clifford Chance LLP), Aaron Karczmer (PayPal), Alfred Kibe (Mastercard), Cindy Levy (McKinsey & Company), Giselle Lim (Takeda Pharmaceutical Company), Domingo Mirón (Accenture), Jody Myers (The Western Union Company), Heike Niebergall-Lackner (International Committee of the Red Cross), Deepak Padaki (Infosys Limited), Hanne Raatikainen (Office of the United Nations High Commissioner for Refugees), Tad Roselund (Boston Consulting Group), Nidhi Seksaria (Mahindra Group), Taalib Shah (Barclays), Lakshmi Shyam-Sunder (World Bank), Richard Smith-Bingham (Marsh McLennan), Matthew Snyder (Centene Corporation), Jacob van der Blij (GAVI), Susan Yasher (Deloitte Touche Tohmatsu Limited) and Yong Seop Yum (SK Group).

*****

A special thanks to experts who contributed to our **thematic** and **regional consultations**.

Chapter 2
Alison Bewick (Nestlé), Jennifer Clazure (World Economic Forum), Dzhangir Dzhangirov (Sberbank), Charles Godfray (Oxford Martin), Brad Hall (Office of Al Gore), Akanksha Khatri (World Economic Forum), Marie Quinney (World Economic Forum), Graeme Riddell (Marsh Advisory) and Nidhi Seksaria (Mahindra Group).

Chapter 3
Paige H. Adams (Zurich Insurance), Kristian Burkhardt (Accenture), Jaya Baloo (Avast Software), Christian Bluhm (UBS AG), Kristian Burkhardt (Accenture), Daniel Dobrygowski (World Economic Forum), Marie-Valentine Florin (International Risk Governance Center), Genevieve Gimbert (PwC), Akshay Joshi (World Economic Forum), Joseph Nocera (PwC), Algirde Pipikaite (World Economic Forum), Rafal Rohozinski (Secdev Group; Zeropoint Security), Vishal Salvi (Infosys), Dmitry Samartsev (BI.ZONE), Scott Stransky (Marsh McLennan) and Effy Vayena (Swiss Federal Institute of Technology).

Chapter 4
Alexander Betts (Oxford University), Bina Desai (Internal Displacement Monitoring Centre), Andrej Kirn (World Economic Forum), Alfredo Malaret (United Nations Institute for Disarmament Research), Marie McAuliffe (International Organization for Migration), Dilip Ratha (World Bank), Miriam Schive (World Economic Forum) and Amali Tower (Climate Refugees).

Chapter 5
Nayef Al-Rodhan (Oxford University), Nikolai Khlystov (World Economic Forum) and Jamie Morin (The Aerospace Corporation).

Europe: 7 July 2021
Alison Bewick (Nestlé), Catherine De Vries (Bocconi University), Katie Henry (Ernest & Young), Louise Marie Hurel (London School of Economics), Joachim Isaacson (UK Armed Forces), Peter Kalotai (European Bank for Reconstruction and Development), Quentin Ladetto (Armasuisse), Pascal Lamy (Jacques Delors Institute), Ian Livsey (Institute for Risk Management), Esther Lynch (European Trade Union), Maurizio Quintavalle (Marsh McLennan), Hanne Raatikainen (Office of the United Nations High Commissioner for

Refugees), Michael Sparrow (World Meteorological Organization), Jacob Van der Blij (GAVI), Lisa Walker (Ecosphere+), Gail Whiteman (University of Exeter Business School) and Susan Wilding (CIVICUS).

Latin America: 13 July 2021
Asdrubal Aguiar Aranguren (Democratic Initiative of Spain and the Americas), Cynthia Arnson (Woodrow Wilson International Center for Scholars), Ricardo Ávila (Portafolio/El Tiempo), Tiago Berriel (Banco BTG Pactual), Luis Bravo (Breca), Antonio de Aguiar Patriota (Government of Brazil), Paula Escobar (La Tercera), Marcela Escobari (Brookings Institution), Luis Fernando Mejía (Fedesarrollo), Mónica Forero (Zurich Insurance), Henrique Fragelli (Nubank), Rafaela Guedes Monteiro (Petroleo Brasileiro), Gerardo Herrera (Marsh McLennan), Enrique Iglesias (AstUr Foundation), Joaquim Levy (Banco Safra), Valeria Moy (Mexican Institute for Competitiveness), Alvin Ortega (Banco Nacional de Panamá), Rafael Palacios Prado (Sociedad de Fomento Fabril), Eric Parrado (InterAmerican Development Bank), Luis Adrián Salazar (University of Costa Rica) and Arturo Sarukhan (Sarukhan + Associates LLC),

North America: 13 July 2021
Tegan Blaine (United States Institute of Peace), David Bloom (Harvard T.H. Chan School of Public Health), Brenda Boultwood (International Monetary Fund), David Bray (Atlantic Council), Jasmina Byrne (UNICEF), Alexis Crow (PwC), Daniel Drezner (The Fletcher School at Tufts University), Jean-Marie Guehenno (Columbia University), Sherri Goodman (Wilson Center), Maha Hosain Aziz (New York University), Aaron Karczmer (PayPal), Carolyn Kousky (Wharton Risk Center), Sonia Kundi (Zurich Insurance Group), Robert Litwak (Wilson Center), Robert Muggah (Igarapé Institute), Lakshmi Shyam-Sunder (World Bank), Adam Tooze (Columbia University), Olivia White (McKinsey & Company) and Michele Wucker (Gray Rhino & Company).

Asia: 21 September 2021
Mushtak Al-Atabi (Heriot-Watt University), Kanti Bajpai (Lee Kuan Yew School of Public Policy, National University of Singapore), Adila Binte Shahrin (Lee Kuan Yew School of Public Policy, National University of Singapore), Tek Yew Chia (Oliver Wyman), Lee Geun (Korea Foundation), Ziad Haider (McKinsey), Yee-Kuang Heng (University of Tokyo), Debora Ianuzzi (Zurich Insurance Group), Peter Jennings (Australian Strategic Policy Institute), Olivia Jensen (Lloyd's Register Foundation Institute for the Public Understanding of Risk), Prakash Kannan (Government of Singapore Investment Corporation), Lynn Kuok (Shangri-La Dialogue), Huong Le Thu (Australian Strategic Policy Institute), Meng Liu (UN Global Compact China), Anita Prakash (Economic Research Institute for ASEAN), Danny Quah (Lee Kuan Yew School of Public Policy, National University of Singapore), Steve Rhee (Ford Foundation), Hersh Shah (Institute of Risk Management, India Affiliate), Lutfey Siddiqi (National University of Singapore, Risk Management Institute), Anjhula Mya Singh Bais (Amnesty International), Louise Tang (Lee Kuan Yew School of Public Policy, National University of Singapore), Chathuni Uduwela (TikTok), Catherine Wong (Lloyd's Register Foundation Institute for the Public Understanding of Risk), Eden Woon (Asian Institute of Technology) and Janson Yap (National University of Singapore).

*****

In addition to those mentioned above, we extend our thanks to the following colleagues for their time and help: Marisol Argueta, Sophie Brown, Diego Bustamante, Eoin Ó Cathasaigh, Arnaud Colin, Roberto Crotti, Ana del Barrio, Attilio di Battista, Beatrice Di Caro, Mirek Dušek, Jaci Eisenberg, Harry Gray Calvo, Kateryna Gordiychuk, Nikhil Kamath, Patrice Kreidi, Gayle Markovitz, Adrian Monck, Nicholai Ozan, Jennifer Perez, Robin Pomeroy, Eduardo Rezende, Katja Rouru, Kirsten Salyer, Miriam Schive, Paul Smyke, Pierre Saouter, Olga Spirina, Jackson Spivey and Vesselina Stefanova Ratcheva.

Design and Production: Thank you to all those involved in the design and production of this year's report. At the World Economic Forum: Sakshi Bhatnagar, Javier Gesto, Floris Landi, Jordynn McKnight, Liam Ó Cathasaigh and Jean-Philippe Stanway. And our external collaborators: Hope Steele (editing) and Andrew Wright (writing and editing). Special thanks to Patrik Svensson for his artistic contributions.

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

The World Economic Forum, committed to improving the state of the world, is the International Organization for Public-Private Cooperation.

The Forum engages the foremost political, business and other leaders of society to shape global, regional and industry agendas.

World Economic Forum
91–93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland

Tel.: +41 (0) 22 869 1212
Fax: +41 (0) 22 786 2744
contact@weforum.org
www.weforum.org

HEFESTIS Weekly Newsletter

A very warm welcome to all of you from all of us at the CISO-Share Office.

We are hosting a member session on Spring4Shell at 10.00am this morning. Invites have already been sent to members and the details and link is also available on the SharePoint site.

Thanks again to all our members who reached out to support the incident reported last month. Recovery is now well underway in very quick time as can be seen from the Heriot-Watt University holding page: https://www.hw.ac.uk/uk/services/is/system-status.htm where further public updates will continue to be provided as they are authorised.

We can only applaud the effectiveness of the response from the entirety of the HW teams and staff who have succeeded in maintaining availability of so many key services for staff, students and stakeholders in the face of a significant attack. Fingers crossed the work continues to go well.

Please check the CiSP site, as always, for the latest updates on current incidents and countermeasures to protect your institution.

Whilst you are there, why not drop into the CISO-Share user forum and discuss the latest topics and news.

Here are a few of the articles which caught the attention of the CISO-Share team this week.

If you have any questions or comments, please feel free to contact us via CISO-Office@hefestis.ac.uk.

Here are some of the week's Cyber Security articles which caught the attention of CISO-Share.

Spring4Shell Information and detection tools

Advisory is similar to the Log4J countermeasures shared in 2021 – Spring's tools are frameworks to help accelerate the development of Java applications and are widely used among Java developers. The bugs being discussed here focus on the Spring Cloud and Spring Framework packages. There has been significant confusion this week about these bugs being the same thing, but they are separate and distinct issues. Both bugs result in the ability to execute arbitrary code on a remote host serving web applications when running vulnerable versions of the software. Obviously, this level of control on a potentially public-facing infrastructure can be extremely impactful. Vulnerabilities are tracked as CVE-2022-22963 and CVE-2022-22965.

Mitigation – patch up affected applications to latest versions of security as updates are released.

Detection tools and analysis

Microsoft detects Spring4Shell attacks across its cloud services
https://www.bleepingcomputer.com/news/security/microsoft-detects-spring4shell-attacks-across-its-cloud-services/

SpringShell (Spring4Shell) Zero-Day Vulnerability CVE-2022-22965 : All You Need To Know
https://jfrog.com/blog/springshell-zero-day-vulnerability-all-you-need-to-know/
Spring has sprung: breaking down CVE-2022-22963 & Spring4Shell (CVE-2022-22965)
https://www.fastly.com/blog/spring-has-sprung-breaking-down-cve-2022-22963-and-spring4shell-cve-2022

Action Point:
Join us this morning at 10:00, the invite has been sent out to members and the event deltails and link are also linked via the CISO-Share SharePoint site.

---

5 ways to improve security hygiene and posture management

https://www.csoonline.com/article/3655629/5-ways-to-improve-security-hygiene-and-posture-management.html

According to ESG research, 80% of organisations plan to increase spending on security hygiene and posture management this year. ESG also asked security professionals to identify actions that could most improve their organisations' security hygiene and posture management. Here are the top responses:

- Performing continuous security control validation to discover gaps in existing security tools (38%).
- Automating processes associated with security hygiene and posture management (36%).
- Deploying a dedicated tool for security/IT asset management that can interoperate and pull data from other existing systems (35%).
- Increasing staff dedicated to security hygiene and posture management (31%).
- Taking a more adversarial/offensive approach to cybersecurity so we can adjust our defences as countermeasures to modern attack TTPs (29%).

Action Point:
These and other suggestions deserve consideration as soon as possible. After all, the growing attack surface won't protect itself.

FBI Shut Down Russia-linked "Cyclops Blink" Botnet That Infected Thousands of Devices

https://thehackernews.com/2022/04/fbi-shut-down-russia-linked-cyclops.html

The U.S. Department of Justice (DoJ) announced that it neutralized **Cyclops Blink**, a modular botnet controlled by a threat actor known as Sandworm, which has been attributed to the Main Intelligence Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU).

The March 22 court-authorized disruption of Cyclops Blink comes a little over a month after intelligence agencies in the U.K. and the U.S. described the botnet as a replacement framework for the VPNFilter malware that was exposed and sinkholed in May 2018.

The company has since revised its Cyclops Blink FAQs to spell out that the vulnerability in question is CVE-2022-23176 (CVSS score: 8.8), which could "allow an unprivileged user with access to Firebox management to authenticate to the system as an administrator" and gain unauthorized remote access.

Action Point:
ASUS has released firmware patches as of April 1, 2022, to block the threat, recommending users to update to the latest version.

PCI Data Security Standard v4.0

https://www.csoonline.com/article/3656608/new-pci-data-security-standard-v40-receives-kudos-for-flexibility.html

Organisations have two years to digest the new standard and make any changes from the current standard, PCI DSS 3.21, which will be retired on March 31, 2024. Key elements in the new standard include:

- Updated firewall terminology to network security controls to support a broader range of technologies used to meet the security objectives traditionally met by firewalls
- Expansion of Requirement 8 to implement multi-factor authentication (MFA) for all access into the cardholder data environment

- Increased flexibility for organizations to demonstrate how they are using different methods to achieve security objectives
- Addition of targeted risk analyses to allow entities the flexibility to define how frequently they perform certain activities, as best suited for their business needs and risk exposure

Action Point:
Make yourself aware of the new changes that are to become part of the contractual agreements that our organisations hold in order to process credit card payments and what changes are needed to ensure continued compliance.

New security features for Windows 11 will help protect hybrid work

https://www.microsoft.com/security/blog/2022/04/05/new-security-features-for-windows-11-will-help-protect-hybrid-work/

This article takes a look at what's coming to Windows 11 to combat the biggest security challenges of distributed work scenarios and the threat landscape of the future. The list includes:

Microsoft Pluton
Built on Zero Trust principles and allowing firmware management to be managed as part of Windows Update.

Smart App Control
Smart App Control only allows processes to run that are predicted to be safe based on either code certificates or an AI model for application trust within the Microsoft cloud.

Enhanced phishing detection and protection with Microsoft Defender SmartScreen
Identifying and alerting users when they are entering their Microsoft credentials into a malicious application or hacked website.

There are many more featured detailed in this article from Microsoft. Some of which will need new installations or resets for existing Windows 11 devices.

Action Point:
Keep abreast of the new security features available for Windows 11 and evaluate whether there is benefit from planning migrations earlier than scheduled.

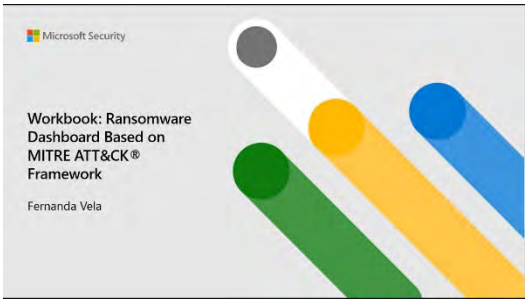
Microsoft 365 Licensing

https://m365maps.com/Microsoft 365 Education.htm

Whilst discussing the security implications of a change in M365 licensing I was directed to the following resource that really helped me to understand the different licencing models that Microsoft has in place for M365.

It's a great resource that can help organisations understand what they currently have access to through their existing licensing model, but also assists in making future decisions on what benefits a licensing uplift will bring in terms of security features and services. I particularly like how each of the boxes allows you to click through to the Microsoft site which is related to that service.

Action Point:
Use this map to realise the full benefits of your organisational M365 licensing model and to plan for future licensing decisions.



New Ransomware Recommendation Dashboard in Microsoft Defender for Cloud

https://techcommunity.microsoft.com/t5/microsoft-defender-for-cloud/new-ransomware-recommendation-dashboard-in-microsoft-defender/ba-p/3270472

For those that have access to Defender for Cloud (A5) Microsoft have released a new dashboard and workbook for prioritising security recommendations to reduce the likelihood of being compromised by a Ransomware attack.

By understand in which stage of the MITRE ATT&CK matrix the recommendation is located, you can prioritize remediations earlier on and reduce the probability of further damage done by the attacker. The Ransomware dashboard can be utilized to prioritize the remediation of recommendations for scenarios such as:

- Ensures up to date VMs with relevant security patches
- Enable anti-malware on your VMs
- Reduce attack surface by enabling just-in-time access to management ports

Action Point:
If you have an A5 license then investigate the workbook and dashboard to ensure that you reconfigurations give the best protection against a Ransomware attack.

"Browser in the Browser" attacks: A devastating new phishing technique arises

https://www.techrepublic.com/article/browser-in-the-browser-attacks-arise

A phishing technique called Browser in the Browser (BITB) has emerged, and it's already aiming at government entities, including Ukraine. Find out how to protect against this new threat.

Phishing for credentials is a common threat that has been around for many years. It uses different social engineering techniques to persuade an unsuspecting user to click on a link or open a document and provide their credentials, which are then sent to the attacker. Now a new phishing technique has been exposed recently by a penetration tester and security researcher known as "mr.d0x" on their website.

What are BITB attacks?
Browser in the browser attacks consist of simulating a browser window within the browser to spoof a legitimate domain. The attack takes advantage of third parties' single sign-on (SSO) option, which has become increasingly common for users to log into many different websites. The principle is pretty straightforward: The user connects to a website, which in turn opens a new browser window

that asks for Google, Apple, Microsoft or other third parties' credentials, to allow the user to log in This benefits the user because they don't need to remember or use an additional password to log into the website.

Action Point:

Recommendations
It seems unreasonable to ask users not to use SSO anymore. They have gotten used to it and it works nicely in most cases. Adding multi-factor authentication (MFA) is a good way to improve security for SSO authentication, yet it could still be bypassed by attackers, by using malware, for example. When it comes to increasing security in phishing cases, the best MFA solutions are hardware devices or tokens.

The use of password managers might also help in the particular case of the BITB attacks. Since the phishing page is in fact not a real browser window, password managers with autocomplete options might not react to them, alerting the user who will wonder why the autocomplete function does not work.

The best ways to avoid BITB attacks are actually the same as for usual phishing. Users should not click on links or attached files coming from unknown sources via email or instant messaging software. If they have doubts about an email coming from a seemingly legitimate entity or colleague, the user should call and verify they were indeed the sender and that the shared link or file is safe.

Anti-phishing solutions should also be deployed and used. If possible, those solutions should allow the user to easily report to the IT department or even to anti-phishing organizations.

Russian Wiper Malware Likely Behind Recent Cyberattack on Viasat KA-SAT Modems

https://thehackernews.com/2022/04/russian-wiper-malware-responsible-for.html

SentinelOne said it uncovered a new piece of malware (named "ukrop") on March 15 that casts the cyberattack aimed at Viasat and temporarily knocked KA-SAT modems offline on February 24, 2022 in a fresh light – a supply chain compromise of the KA-SAT management mechanism to deliver the wiper, dubbed **AcidRain**, to the modems and routers and achieve scalable disruption.
AcidRain is an executable that "performs an in-depth wipe of the filesystem and various known storage device files,". Once the wiping process is complete, the device is rebooted to render it inoperable.

This makes AcidRain the seventh wiper strain to be uncovered since the start of the year in connection with the Russo-Ukrainian war after:
WhisperGate, WhisperKill, HermeticWiper, IsaacWiper, CaddyWiper, and DoubleZero.

Action Point:

The use of wipers is becoming a more common occurrence due to the war in Ukraine. There are elements within the code of this wiper that points to Russian based attackers. Ensure that recovery processes address the possibility of complete loss of services requiring a rebuild from scratch.

All the best from all of us at **HEFESTIS** and look out for our next **Threatscape** update next week.

HEFESTIS Weekly Newsletter

A very warm welcome to all of you from all of us at the CISO-Share Office.

Thanks again to all our members who reached out to support the incident reported last month. Recovery is now well underway in very quick time as can be seen from the Heriot-Watt University holding page: https://www.hw.ac.uk/uk/services/is/system-status.htm where further public updates will continue to be provided as they are authorised.

We can only applaud the effectiveness of the response from the entirety of the HW teams and staff who have succeeded in maintaining availability of so many key services for staff, students and stakeholders in the face of a significant attack. Fingers crossed the work continues to go well.

Please check the CiSP site, as always, for the latest updates on current incidents and countermeasures to protect your institution.

Whilst you are here, why not drop into the CISO-Share user forum and discuss the latest topics and news.

Articles which may be of interest covering Zero Trust, more on the Lapsus$ group, vulnerabilities, phishing kits and much more are included with this week's issue.

The Chaos (and Cost) of Lapsus$ Hacking Carnage

Security experts say the Lapsus$ gang's "extortion and destruction" hacking spree is the work of an amateur gang allegedly led by a British teenager. What does this say about the state of cybersecurity?

Main Article

Microsoft, Okta Confirm Data Breaches Involving Compromised Accounts

Lapsus$ Claims Hack of IT Giant Globant After Arrests of Alleged Members

The timing for Lapsus$ attacks couldn't possibly be worse.

As enterprise network defenders absorbed warnings about cyberwar and confirmed reports of nation-state wiper and ransomware attacks, the Lapsus$ hacking gang stormed into public view with taunts and evidence of data-theft hacks against prominent brands NVIDIA, Samsung and Ubisoft.

Later, Microsoft and Okta would be dragged into the victim pool with Redmond publicly documenting "a large-scale social engineering and extortion campaign" and Okta badly botching its communications with customers on the extent of its breach.

Action Point: "Keep in mind, there are no fancy zero-days involved. They're [Lapsus$] is showing that you don't have to use zero-days or clever exploits. They're exploiting an entire system where data is flowing everywhere and we really don't have the controls to manage it."

Microsoft recommends that organizations adopt inside risk-management playbooks to mitigate damage from social engineering and identity-centric tactics used by the Lapsus$ gang.

These include the mandatory use of MFA (multi-factor authentication) technology for all users from all locations, including even perceptive trusted environments. The MFA rollout should also include all inter-facing infrastructure, even those coming from on-prem locations.

Redmond is also urging businesses to use modern authentication options (OAuth or SAML connected to Azure AD) to enable risk-based sign-in detection, and to strengthen and monitor cloud security deployments for signs of malicious activity.

The Need for Resilient Zero Trust

It is essential to ensure that any Zero Trust technology used is resilient to external factors

Main Article

The growing threat of cyberattacks like SolarWinds, JBS USA, and Colonial Pipeline has underscored that organizations can no longer depend on conventional perimeter-based defenses to protect critical systems and data. The Log4j vulnerability is the latest sign that organizations must assume that cyber adversaries are already in their network. Against the backdrop of these high-profile incidents and growing concerns of retaliatory cyberattacks by Russia following its invasion of Ukraine, legislators have stepped up their efforts to bolster resilience and response capabilities against these threats (e.g., U.S. Cyber Incident Reporting for Critical Infrastructure Act, European Union Rules for Common Cybersecurity and Information Security Measures).

Action Points: Considering these benefits, more and more cyber risk and security management frameworks are adopting the concept of cyber resilience. For example, the Department of Homeland Security's Cyber Resilience Review (CRR) offers guidance on how to evaluate an organization's operational resilience and cybersecurity practices. Another example is the National Institute of Standards and Technology (NIST) Special Publication 800-160 Volume 2, which offers a framework for engineering secure and reliable systems—treating adverse cyber events as both resilience and security issues.

Ultimately, cyber resilience is the only way to guarantee true Zero Trust. When implemented properly, resilient Zero Trust becomes a preventive measure that counteracts human error, malicious actions, and decayed, insecure software.

Microsoft Is Adding A New Driver-Blocklist Feature To Windows Defender On Windows 10 And 11

Microsoft is adding a new security option to Windows Defender that is meant to help protect against malicious drivers on Windows 10 and 11 devices.

Main Article

The feature will be enabled by default on Windows 10 in S Mode, as well as on devices that have the Memory Integrity Core Isolation feature, which relies on virtualization-based security. (This Core Isolation Memory Integrity feature also is known as Hypervisor-protected Code Integrity or HVCI). More details are available in this Microsoft article about recommended driver block rules.

Learning Point: In other security-related news, Microsoft announced plans for a new U.S. Government cloud environment -- Office 365 Government Secret -- on March 28. Currently in government review, this new Secret cloud is designed for the U.S. Federal Civilian, Department of Defense (DoD), Intelligence Community (IC), and U.S. Government partners working within Secret environments with Microsoft's Software as a Service (SaaS) capabilities for all data classifications. The Office 365 Government Secret cloud environment is built on Microsoft's Azure Government classified environments.

Cybercriminals' Phishing Kits Make Credential Theft Easier Than Ever

Phishing attempts are within reach of less tech-savvy attackers, thanks to the rise of phishing kits. Learn where these kits are found, how they work, and how to combat them.

Main Article

Kaspersky recently published research about phishing kits. These kits are complete packages sold or provided to cybercriminals. Those kits often include manuals and documentation to help fraudsters use it.

The most basic offer consists of a single web page and a script to store the stolen data locally (i.e., in a hidden folder) or send the data to a remote location via email or third-party communication software, like Telegram.

Action Points: Recommendations for phishing kit defense

- **Do not click on links or attached files contained in emails coming from unknown sources, or in any communication software like Telegram, WhatsApp, etc.**
- If an email seems to come from a colleague but has somehow unusual characteristics (email footer missing, spelling mistakes, etc.) call the colleague and verify that they were indeed the sender and that you can click on the link or open the attached file safely.
- Make sure the URL the link leads to is correct and legitimate.
- Be aware that SMS on mobile phones might also contain links to phishing pages. Do not click on any link coming from an unknown source, or even from a seemingly legitimate one if you did not expect an SMS from it.
- If you get a message that seems legitimate from an entity, go to its website and log in rather than using the link provided in the email.
- Be aware that browsing a website using HTTPS does not mean it is safe. More and more cybercriminals use free SSL certificates for their phishing domains.
- Use anti-phishing solutions to protect your browser from phishing websites.
- Report phishing websites you might detect to your IT department or even to anti-phishing organizations. This will help everyone on the internet since it is generally quickly addressed by blocking software.

CISA Adds 66 Vulnerabilities To List Of Bugs Exploited In Attacks

The Cybersecurity and Infrastructure Security Agency (CISA) has added a massive set of 66 actively exploited vulnerabilities to its catalog of 'Known Exploited Vulnerabilities.'

Main Article

The list shows us how quickly threat actors begin targeting a vulnerability once a vendor discloses it.

For example, the Windows Print Spooler CVE-2022-21999 vulnerability, the Mitel DDoS CVE-2022-26143 amplification vulnerability, and the CVE-2022-26318 WatchGuard vulnerabilities were disclosed in February and were quickly exploited by threat actors.

Due to this, it is critical for admins to apply security updates as soon as possible to prevent their exploitation, especially on internet-exposed devices.

These flaws have been observed in real cyberattacks against organizations, so they are published to raise awareness to system administrations and serve as official advisories for applying the corresponding security updates.

In this case, CISA gives federal agencies until April 15, 2022, to patch the listed vulnerabilities and reduce the risk of falling victim to cyberattacks.

Action Point: The new set of 66 actively exploited vulnerabilities published by CISA spans disclosure dates between 2005 and 2022, covering a broad spectrum of software and hardware types and versions.

Due to the large number of flaws comprising the latest set, CISA hasn't supplied the usual summary table, so system administrators will have to review the new entries on the catalogue, which now counts a total of 570 vulnerabilities.

Once at the catalogue, you can click on the 'Date Added' column header to sort by the most recently added vulnerabilities.

Resolved RCE in Sophos Firewall

An authentication bypass vulnerability (CVE-2022-1040) allowing remote code execution was discovered in the User Portal and Webadmin of Sophos Firewall v18.5 MR3 (18.5.3) and older.

Support Article

There is no action required for Sophos Firewall customers with the "Allow automatic installation of hotfixes" feature enabled. Enabled is the default setting.

Customers can protect themselves from external attackers by ensuring their User Portal and Webadmin are not exposed to WAN.

There are a number of fixes available:

> Hotfixes for v17.0 MR10 EAL4+, v17.5 MR16 and MR17, v18.0 MR5(-1) and MR6, v18.5 MR1 and MR2, and v19.0 EAP published on March 23, 2022
>
> Hotfixes for unsupported EOL versions v17.5 MR12 through MR15, and v18.0 MR3 and MR4 published on March 23, 2022
>
> Hotfixes for unsupported EOL version v18.5 GA published on March 24, 2022
>
> Hotfixes for v18.5 MR3 published on March 24, 2022
>
> Fix included in v19.0 GA and v18.5 MR4 (18.5.4)

Users of older versions of Sophos Firewall are required to upgrade to receive the latest protections and this fix

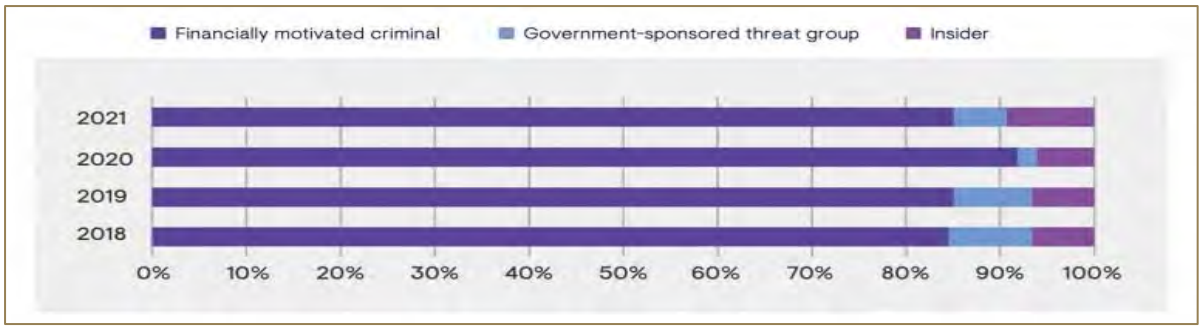
Learning Points:
Something that should be looked at closely as the benefits of an effective data management strategy include reduced IT costs, easier data sharing, better security, less legal exposure, and an improved ability to demonstrate governance and regulatory compliance.

Lessons Learned From 2021

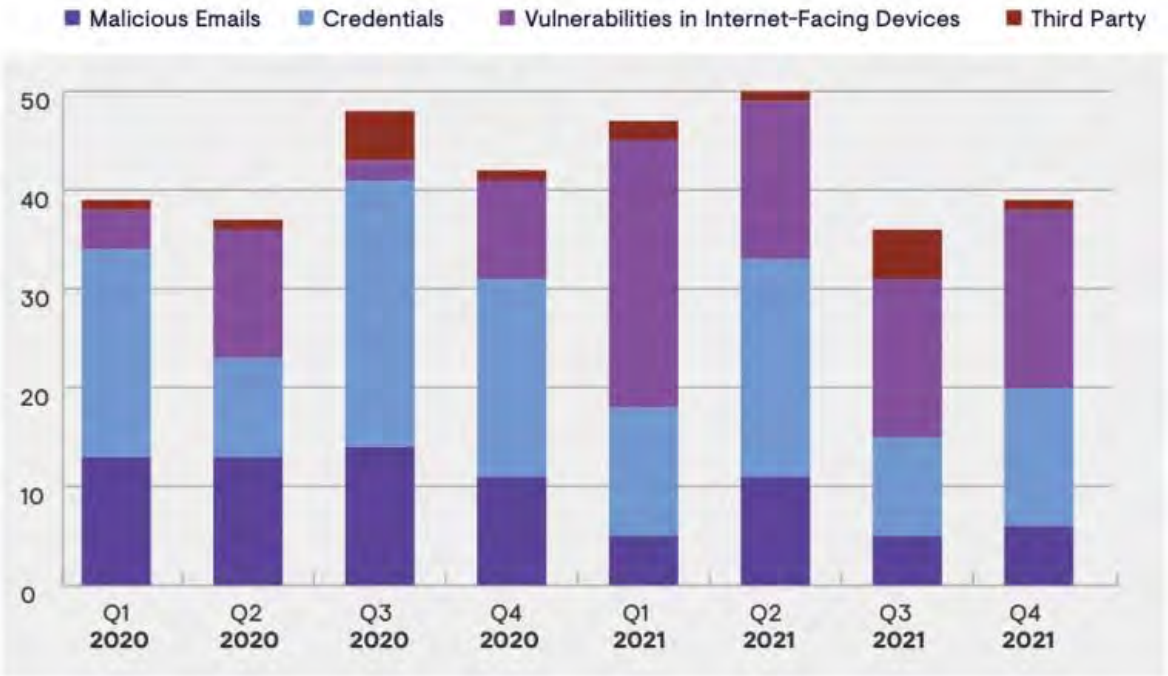
SecureWorks covered more than 450 security incidents in 2021 and published its feedback on it.

Main Article

A large 85% of incidents handled by SecureWorks in 2021 were financially oriented, while government-sponsored threat attacks only represented 5% of the activity. About 9% remaining consists of deliberate or accidental actions from employees that caused security incidents.



Forty-three percent of the initial access was gained by threat actors by exploiting vulnerabilities in internet-facing devices.



Learning Points: SecureWorks provides a top 20 recommendations in its report including:

- Performing regular vulnerability scans
- Monitor for newly registered spoofed domains on the internet
- Control access carefully and make IP address allow lists
- Improve backup strategies and procedures
- Implement MFA
- Implement DKIM and SPF authentication for email.

How To Create A Security Program

When creating a security program this article suggests focusing attention on the following perspectives.

Main Article

When creating a security program this article suggests focusing attention on the following perspectives.

1. Business awareness
Understanding business goals, products, services, challenges, and strategies help the security team do their traditional tasks while supporting business objectives, and also enabling the assessment of risk to make smart decisions based on the business and cybersecurity landscape.

2. Strategic positioning
Understanding the kind of value the information security program can provide to the business is essential for the buy-in and support of your program.

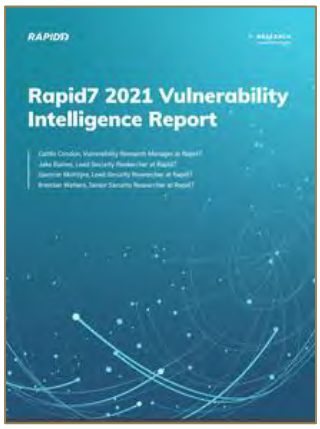
3. Engagement
The security program should not be a one-person challenge. The department should engage everyone who can contribute to disseminating the security culture across the organization.

4. Build a strong team
Having a challenged, passionate, and skilled team will help drive any technical changes that should be addressed while keeping stakeholders and the entire organisation connected to the strategy. A strong team also represents the needed technical know-how the organization will have to better manage risks.

5. Communication
Communication is the key link between giving the right message and listening to what is being communicated. Changes take time and require continued interactions to make them sustainable.

Action Point:

Consider that the security department should be an important part of the organisation that is resilient and adaptable to change. This way, whatever happens internally or the risk landscape, security will continue to play its part in enabling business.



Rapid7 2021 Vulnerability Intelligence Report

Security, IT, and other teams tasked with vulnerability management and risk reduction operate in high-urgency, high-stakes environments where informed decision-making hinges on the ability to quickly separate signal from a sea of perpetual noise.

Rapid7 2021
Vulnerability Intelligei

When a new potential threat emerges, information security professionals often find themselves needing to translate vague descriptions and untested research artifacts into actionable intelligence for their own particular risk models. Rapid7 researchers analyze thousands of vulnerabilities each year to understand root causes, dispel misconceptions, and share information on why certain flaws are more likely to be exploited than others.

This report examines notable vulnerabilities and high-impact attacks from 2021 in order to highlight exploitation trends, explore attacker use cases, and offer a framework for understanding new security threats as they arise. Our aim is to contextualize the vulnerabilities that introduce serious risk to a wide range of organizations—in order to separate them from those that probably don't. We have also included a section with meaningful guidance for defenders.

Learning Point: Rapid7's 2021 Vulnerability Intelligence Report examines 50 vulnerabilities that pose considerable risk to organizations of all sizes. In total, this report includes 43 vulnerabilities that were exploited in the wild in 2021, almost half of which arose from zero-day exploits.

We also highlight a number of non-CVE-based attacks, including several significant supply chain security incidents.

See appendix for additional context on vulnerability selection.

All the best from all of us at **HEFESTIS** and look out for our next **Threatscape** update next week.

RESEARCH

Rapid7 2021 Vulnerability Intelligence Report

Caitlin Condon, Vulnerability Research Manager at Rapid7
Jake Baines, Lead Security Researcher at Rapid7
Spencer McIntyre, Lead Security Researcher at Rapid7
Brendan Watters, Senior Security Researcher at Rapid7

TABLE OF CONTENTS

Executive Summary 4

Big Picture 6

2021 Exploited and Significant Vulnerabilities 9

- Time to Exploitation 10
- Widespread Threats 11
- Other Known Exploited Vulnerabilities 16
- Impending Threats 18

2021 Attack Trends 21

- Attacker Utilities and Vulnerability Classes 21
- A Little Goes A Long Way: Server-Side Request Forgery 22
- Attack Chains 24
- Bring Your Own Vulnerable Driver (BYOVD) 26
- Chain Reaction: Present and Future Software Supply Chain Risk 27

Spotlight: Key 2021 Windows Vulnerabilities 29

- Evacuate the (On) Premises: We Need to Talk About Exchange 29
- Nightmares and Novelties 30

Practical Guidance for Defenders 33

Appendix 36

- Full Dataset 36
- Notes on Methodology 40
  - Threat Categorization 41
  - Ransomware Citations 41
  - Calculating Time to Known Exploitation (TTKE) 41
- Glossary of Terms 42
  - Attacker Utilities 42
  - Vulnerability Classes 42

References 44

Executive Summary

Security, IT, and other teams tasked with vulnerability management and risk reduction operate in high-urgency, high-stakes environments where informed decision-making hinges on the ability to quickly separate signal from a sea of perpetual noise. When a new potential threat emerges, information security professionals often find themselves needing to translate vague descriptions and untested research artifacts into actionable intelligence for their own particular risk models.

Rapid7 researchers analyze thousands of vulnerabilities each year to understand root causes, dispel misconceptions, and share information on why certain flaws are more likely to be exploited than others. This report examines notable vulnerabilities and high-impact attacks from 2021 in order to highlight exploitation trends, explore attacker use cases, and offer a framework for understanding new security threats as they arise. Our aim is to contextualize the vulnerabilities that introduce serious risk to a wide range of organizations—in order to separate them from those that probably don't. We have also included a section with meaningful guidance for defenders.

Rapid7's 2021 Vulnerability Intelligence Report examines 50 vulnerabilities that pose considerable risk to organizations of all sizes. In total, this report includes 43 vulnerabilities that were exploited in the wild in 2021, almost half of which arose from zero-day exploits. We also highlight a number of non-CVE-based attacks, including several significant supply chain security incidents. See our appendix for additional context on vulnerability selection.

2021 findings include:

- Broad, opportunistic exploitation increased dramatically. A widespread threat is a vulnerability that is exploited by many malicious actors or used in at-scale attacks like ransomware operations; we differentiate widespread attacks from other exploited vulnerabilities to emphasize higher risk to corporate networks. Rapid7's vulnerability research team tracked 33 net-new widespread threats in 2021, a 136% rise in widespread threats from 2020.
- 21 of the vulnerabilities in this report are known to have been exploited to carry out ransomware attacks.
- Zero-day attacks increased significantly: This report includes 20 vulnerabilities that were exploited in the wild as zero-days before vendors were able to patch them—double the number of zero-day attacks in our 2020 dataset. More than half of all the widespread threats Rapid7 researchers analyzed in 2021 began with a zero-day exploit.
- The window between when a vulnerability is publicly disclosed and when it is known to be exploited in the wild ("time to known exploitation," or TTKE) decreased. 50% of the CVEs in this report were exploited within seven days of public disclosure, compared with 30% in 2020. The rise in widespread zero-day attacks in 2021 was the main driver of reduced time to exploitation; shorter TTKE has also meant that organizations' incident response and emergency patch procedures were put to the test, and any security or IT team who didn't have these protocols in place was at a considerable disadvantage.

Notable attack vectors and other exploitation trends in 2021 include:

- An influx of injection attacks (including server-side request forgery bugs), a steady uptick in driver-based attacks, and continued validation of relaying as an attack technique of choice for penetration testers and adversaries alike.
- High-profile attacks on CI/CD tooling, widely used open-source libraries, and upstream service providers, all of which contributed to ongoing fears about threats to software supply chain integrity.

The full dataset is available in the appendix.

Big Picture

In the last two weeks of 2020, after news broke that Texas-based IT company SolarWinds had been the victim of a supply chain compromise that resulted in a backdoored version of their Orion monitoring software being shipped to thousands of customers worldwide, a litany of businesses and government agencies disclosed follow-on breaches and shared technical analysis and threat indicators from their own internal investigations. In some ways, the outpouring of research and intelligence artifacts from prominent security and technology firms in the wake of the SolarWinds revelations made for a remarkable period of information sharing as the industry's understanding of the attack evolved throughout the early months of 2021. In other ways, the SolarWinds supply chain hack underscored, with renewed urgency, the risk posed by our collective reliance on popular technologies and legacy code bases that often sit in critical, privileged positions in organizations' networks.

The threat landscape in 2021 brought historical security lessons to bear in novel, pressing ways even as the lingering pall of the COVID-19 pandemic drove staffing and budget constraints across organizations of all sizes. A rise in attack complexity as well as severity further compounded the challenges security teams faced in 2021: In the six weeks immediately following confirmation of the SolarWinds supply chain compromise, for example, there were at least two dozen additional SolarWinds-related developments that prompted action from security practitioners who scrambled to evaluate new vendor breach statements, deploy zero-day patches, and operationalize fresh indicators of compromise.

Almost exactly a year after the SolarWinds supply chain compromise took over news headlines, the security community found itself in the middle of remediation and detection efforts for what can reasonably be called the single biggest cybersecurity incident in history. The Log4Shell vulnerability—CVE-2021-44228, a perniciously simple JNDI injection flaw in Apache's widely deployed open-source Log4j logging library—is present in everything from web and email servers to mobile applications and cloud services and allows remote, unauthenticated attackers to take control of vulnerable targets with a single-line request.

Log4Shell made for a stark contrast to the SolarWinds incident: Public awareness began with warnings from the **Minecraft** gaming community rather than with National Security Council **meetings** at the White House. There were no high-gloss headlines about **Russia** and espionage, no bespoke **stellar-themed malware names** in capital letters. Far from making millions from Fortune 500 **customers**, Log4j is maintained by a very few **unpaid open-source developers**. Moreover, the SolarWinds incident was a long-term targeted incursion by a single threat actor, albeit an advanced one. Log4Shell marked the beginning of a free-for-all that offered both advanced and low-skilled adversaries open shots on target machines, many of which are internet-facing by design or necessity.

CVE-2021-44228 is a resolutely technical and deeply unsexy vulnerability—a key factor for security teams whose jobs suddenly included convincing IT and business stakeholders to embark upon massive patching and remediation operations two weeks before end-of-year holidays. Log4Shell's lack of shine and lower accessibility to business audiences also helps cement a likely part of its legacy: Detection and patching difficulty combined with large attack surface area meant that skilled adversaries had abundant opportunities to gain footholds and establish persistence in corporate networks, reducing the barrier to entry for future exploits against internal systems that might otherwise have required an extra step to obtain network access.

All in all, 2021 was frenetic and rather bleak for many risk management teams, even before Log4Shell demanded round-the-clock mitigation efforts at a time when many companies had already implemented year-end code freezes. Widespread attacks leveraging vulnerabilities in commonly deployed software were endemic, ransomware prevalence continued to increase sharply, and zero-day exploitation reached what is generally thought to be an **all-time high**. The window between public vulnerability disclosure and observed attacks has narrowed, straining patching timelines and incident response capabilities. And community concern over supply chain and open-source security has proven well-founded amid high-profile attacks on popular **libraries** and **developer tools**.

The threat landscape in 2021 brought historical security lessons to bear in novel, pressing ways even as the lingering pall of the COVID-19 pandemic drove staffing and budget constraints across organizations of all sizes.

There are, however, some glimmers of good news coming out of what felt like a grim year overall. For one thing, the security industry is able to measure the huge spike in zero-day attacks in large part because zero-day exploits are being better detected and analyzed, which has benefited both commercial security tooling and open-source rulesets.

The rise in ransomware has spurred significant **public-private cooperation** and driven new recommendations for more effectively deterring and responding to ransomware attacks. Public alerting from world governments and industry bodies matured, too: In November 2021, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) published **a catalog** of nearly 300 known-exploited vulnerabilities (100+ of which are from 2021), accompanied by a **binding** operational directive instructing federal agencies to remediate within certain time frames.

Within this report, we look at the vulnerabilities that introduced risk to many organizations irrespective of size, maturity, or industry vertical. Our primary concern when defining the CVEs and metadata we have included within is not who was doing the attacking—although we have made an exception for ransomware operators—but rather the volume of attacks being levied against any particular flaw or attack surface. We strongly recommend prioritizing remediation for the CVEs in this year's dataset on an urgent basis.

“There are, however, some glimmers of good news coming out of what felt like a grim year overall.

2021 Exploited and Significant Vulnerabilities

Rapid7 vulnerability researchers prioritize CVEs that are likely to impact many organizations, instead of those likely to affect only a few. We intentionally differentiate mass attacks from smaller-scale or targeted exploitation; when a vulnerability is exploited by many attackers across many different industries and organizations, we deem that vulnerability a **widespread threat**. As a rule, organizations should expect to conduct incident response investigations that look for IOCs and post-exploitation activity during widespread threat events in addition to activating emergency patching protocols.

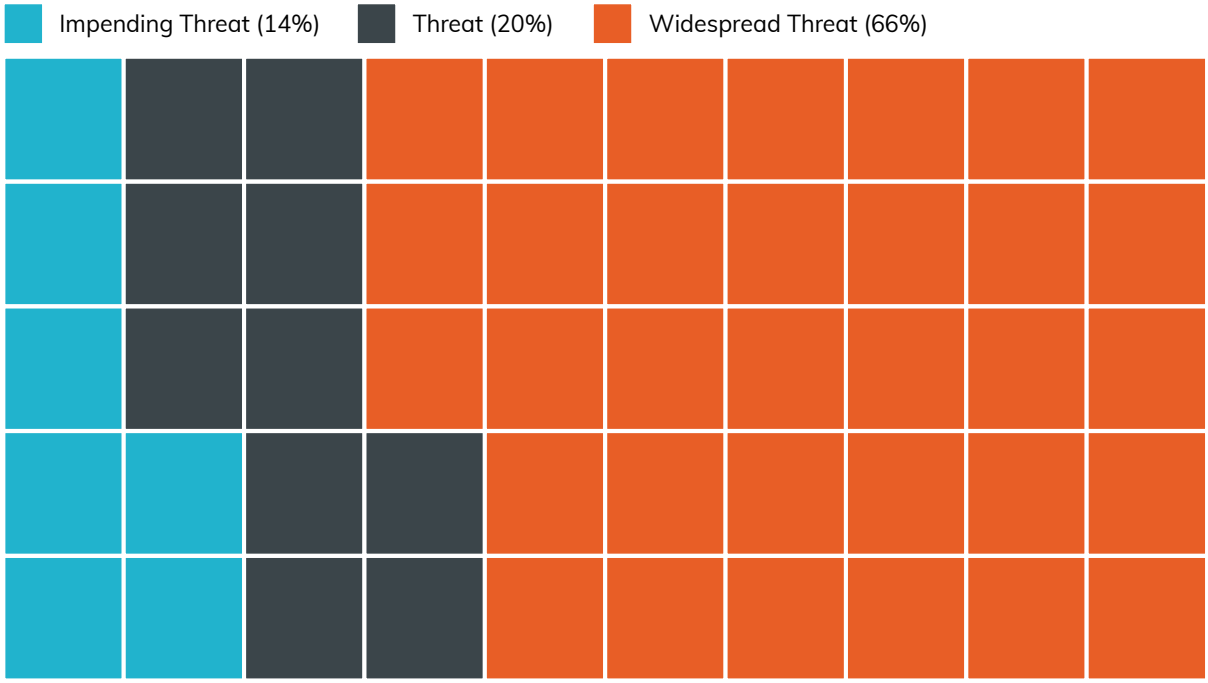
Vulnerabilities categorized as **threats** have been reported as exploited in the wild by reputable sources (including Rapid7's own Labs and services teams), but in a more limited or targeted fashion than CVEs classified as widespread threats. Impending threats, on the other hand, have not yet seen exploitation by adversaries, but in our view are likely and valuable attack targets.

In contrast with 2020, the majority of the CVEs we analyzed in 2021 were classified as widespread threats. Because the volume of attacks increased so much, impending threats fell from 40% of our vulnerability dataset in 2020 to only 14% in 2021.

What is a threat?

When there is an adversary with the intent, capability, and opportunity, a threat exists. When two or more of these elements are present (e.g., intent and capability, but no opportunity), we call it an impending threat, because there is just one missing piece before it becomes a true threat. When there is just one element present (e.g., an opportunity in the form of a software vulnerability), we call it a potential threat. There is the potential for it to turn into a true threat, but there are additional components that need to come to fruition before it has a real impact to most organizations.

2021 Vulnerabilities by Threat Status



Time to Exploitation

One of the key metrics Rapid7 research teams track is the time between when vulnerabilities we analyze become known to the public and when they are reported as exploited in the wild. This window, which we call "Time to Known Exploitation" (TTKE), has shrunk over the past year, largely owing to the surge of widespread zero-day attacks. 50% of the vulnerabilities in this report were exploited within seven days of public disclosure, and 58% were exploited within two weeks. By contrast, only 30% of the vulnerabilities we included in our 2020 report were exploited within a week and 32% within two weeks.

Overall, the average time to known exploitation for vulnerabilities in this report is 12 days in 2021 compared with 42 days for vulnerabilities in our 2020 report—a 71% decrease.

As we outline in the section below, a rise in zero-day exploitation was the primary driver of a narrow (or negative) window between disclosure and in-the-wild attacks. But whatever the cause, lower TTKE has serious implications for organizations' security programs. A drastic reduction in time to exploitation year over year means that not only are well-worn emergency patching procedures necessary, incident response protocols are likely to require repeated use as well. Down time was a red flag for many businesses even years ago; in the modern "five nines" world of SaaS models, disruptive maintenance is at best a negotiation, and at worst an instant deal breaker for many companies. Effective prioritization and understanding of internet exposure are critical capabilities for security teams whose day-to-day operations have grown to include *communicating* risk as much as remediating it.

Overall, the average time to known exploitation for vulnerabilities in this report is 12 days in 2021 compared with 42 days for vulnerabilities in our 2020 report—a 71% decrease.

Widespread Threats

2021 witnessed a significant increase in broad, opportunistic exploitation of severe vulnerabilities, driven in-part by attacker economies of scale like ransomware operations and coin mining campaigns. In one of the year's most jarring trends, 52% of 2021's widespread threats began with a zero-day exploit—exploited in the wild by threat actors before the vendors made patches available. This is both unusual and wildly alarming: It's common to see zero-day exploitation in highly targeted attacks, as we did in 2020, but a huge percentage (85%) of 2021's zero-day exploits threatened many organizations from the outset instead of only a few.

We tracked 33 widespread threats that compromised many organizations in 2021, but increasingly, the proliferation of ransomware affiliates and other commodity attacks means that additional vulnerabilities are likely to be weaponized at scale, too. Just under two thirds (64%) of 2021's widely exploited vulnerabilities are known to have been leveraged by ransomware groups.

CVE	Threat Status	Attacker Utility	Vulnerability Class	Time to Known Exploitation (TTKE) in Days	Ransomware?
CVE-2020-6207 SAP Solution Manager Missing Authentication Check	• Widespread Threat (0day)	Network infrastructure compromise	Improper Access Control	Unknown	Unconfirmed
CVE-2020-29583 Zyxel USG Hardcoded Admin Credential	• Widespread Threat (0day)	Network pivot	Improper Access Control	14	Unconfirmed
CVE-2021-20016 SonicWall SMA 100 Series Unauthenticated SQL Injection	• Widespread Threat (0day)	Network pivot	Injection / SQL	0	Yes
CVE-2021-27103 Accellion FTA Server-Side Request Forgery	• Widespread Threat (0day)	Remote code execution	Injection / Request	0	Yes**
CVE-2021-27101 Accellion FTA Unauthenticated SQL Injection	• Widespread Threat (0day)	Remote code execution	Injection / SQL	0	Yes**
CVE-2021-21972 VMware vCenter Server Remote Code Execution	• Widespread Threat (0day)	Network infrastructure compromise	Improper Access Control	7	Yes

CVE	Threat Status	Attacker Utiliity	Vulnerability Class	Time to Known Exploitation (TTKE) in Days	Ransomware?
CVE-2021-26857 Microsoft Exchange Server Unified Messaging Deserialization "ProxyLogon"	• Widespread Threat (0day)	Remote code execution	Deserialization	0	Yes
CVE-2021-26858 Microsoft Exchange Server Arbitrary File Write "ProxyLogon"	• Widespread Threat (0day)	Remote code execution	Injection / File	0	Yes
CVE-2021-27065 Microsoft Exchange Server Arbitrary File Write "ProxyLogon"	• Widespread Threat (0day)	Remote code execution	Injection / File	0	Yes
CVE-2021-26855 Microsoft Exchange Server-Side Request Forgery "ProxyLogon"	• Widespread Threat (0day)	Remote code execution	Injection / Request	0	Yes
CVE-2021-22986 F5 iControl REST Unauthenticated Remote Command Execution	• Widespread Threat	Network pivot	Injection / Command	9	Unconfirmed
CVE-2021-20021 SonicWall Email Security Pre-Authentication Administrative Account Creation	• Widespread Threat (0day)	Network pivot	Improper Access Control	0	Yes
CVE-2021-22205 GitLab Unauthenticated Remote Code Execution	• Widespread Threat	Remote code execution	Improper Access Control	48	Yes
CVE-2021-22893 Pulse Connect Secure Remote Unauthenticated Arbitrary Code Execution	• Widespread Threat (0day)	Network pivot	Memory Corruption	0	Yes

CVE	Threat Status	Attacker Utiliity	Vulnerability Class	Time to Known Exploitation (TTKE) in Days	Ransomware?
CVE-2021-28799 QNAP HBS 3 Improper Authorization	• Widespread Threat (0day)	Network pivot	Improper Access Control	0	Yes
CVE-2021-31207 Microsoft Exchange Server Security Feature Bypass "ProxyShell"	• Widespread Threat	Remote code execution	Injection / Request	93	Yes
CVE-2021-21985 VMware vCenter Server Remote Code Execution	• Widespread Threat	Network infrastructure compromise	Injection / JNDI	10	Unconfirmed
CVE-2021-35464 ForgeRock AM Unauthenticated Remote Code Execution	• Widespread Threat	Remote code execution	Deserialization	7	Unconfirmed
CVE-2021-34527 Microsoft Windows Print Spooler Remote Code Execution "PrintNightmare"	• Widespread Threat (0day)	Remote code execution	Improper Access Control	0	Yes
CVE-2021-30116 Kaseya VSA Credential Disclosure	• Widespread Threat (0day)	Information disclosure	Improper Access Control	0	Yes
CVE-2021-35211 SolarWinds Serv-U Remote Memory Escape	• Widespread Threat (0day)	Remote code execution	Memory Corruption	0	Yes
CVE-2021-36942 Microsoft Windows LSA Spoofing "PetitPotam Attack"	• Widespread Threat	Network infrastructure compromise	Improper Access Control	33	Unconfirmed
CVE-2021-26084 Atlassian Confluence Server Webwork OGNL Injection	• Widespread Threat	Remote code execution	Injection / OGNL	7	Yes

CVE	Threat Status	Attacker Utiliity	Vulnerability Class	Time to Known Exploitation (TTKE) in Days	Ransomware?
CVE-2021-40444 Microsoft MSHTML Remote Code Execution	• Widespread Threat (0day)	Remote code execution	Injection / ActiveX	0	Yes
CVE-2021-38647 Microsoft Azure Open Management Infrastructure Remote Code Execution "OMIgod"	• Widespread Threat	Remote code execution	Improper Access Control	2	Unconfirmed
CVE-2021-44077 Zoho ManageEngine ServiceDesk Plus Unauthenticated Remote Code Execution	• Widespread Threat	Remote code execution	Improper Access Control	67	Unconfirmed
CVE-2021-22005 VMware vCenter Server Arbitrary File Upload	• Widespread Threat	Network infrastructure compromise	Injection / File	3	Unconfirmed
CVE-2021-41773 Apache HTTP Server Path Traversal and Remote Code Execution	• Widespread Threat (0day)	Remote code execution	Improper Access Control	0	Unconfirmed
CVE-2021-42237 Sitecore Unauthenticated Remote Code Execution	• Widespread Threat	Remote code execution	Deserialization	28	Unconfirmed
CVE-2021-44515 Zoho ManageEngine Desktop Central Authentication Bypass	• Widespread Threat (0day)	Network infrastructure compromise	Improper Access Control	0	Unconfirmed
CVE-2021-44228 Apache Log4j Unauthenticated Remote Code Execution "Log4Shell"	• Widespread Threat (0day)	Remote code execution	Injection / JNDI	0	Yes

CVE	Threat Status	Attacker Utiliity	Vulnerability Class	Time to Known Exploitation (TTKE) in Days	Ransomware?
CVE-2021-34473 Microsoft Exchange Server Remote Code Execution "ProxyShell"	• Widespread Threat	Remote code execution	Improper Access Control	30	Yes
CVE-2021-34523 Microsoft Exchange Server Elevation of Privilege "ProxyShell"	• Widespread Threat	Local code execution	Improper Access Control	30	Yes

**Conflicting reports on zero-day exploitation. CVE-2021-28799 was patched on April 16, 2021 but not disclosed publicly until April 22. A Qlocker ransomware campaign exploited multiple QNAP CVEs beginning April 19, 2021.*

*** Clop ransomware threat actors leveraged the Accellion FTA zero-day vulnerabilities in an extortion campaign and did not actually deploy ransomware.*

The first widespread threat of 2021 was CVE-2020-29583, a hard-coded admin credential vulnerability in Zyxel firewalls and AP controllers. Echoing 2019's Citrix Netscaler vulnerability, the Zyxel flaw debuted just before Christmas and saw opportunistic exploitation the first week of January. Not long after, Accellion and SonicWall were subjected to sophisticated cyberattacks that used zero-day vulnerabilities in their own products to compromise the organizations themselves and their downstream customers.

The rest of 2021 was punctuated by widespread, high-profile attacks on technology cornerstones like Microsoft Exchange Server, VMware's vCenter Server, and core Windows services. In between, we saw opportunistic exploitation of common enterprise software like Atlassian Confluence, F5's iControl interface, and GitLab servers, along with cyberattacks against security vendors like Ivanti (Pulse Connect Secure) in addition to SonicWall and Accellion. Finally, attackers took potshots against Zoho's expansive ManageEngine suite of products, with widespread threats manifesting against ServiceDesk Plus (CVE-2021-44077) and Desktop Central (CVE-2021-44515), both of which exposed managed service providers (MSPs) in addition to business users.

The impact of successful exploitation for each of these vulnerabilities is high; most allow for remote code execution (RCE) at a minimum, but several allow unauthenticated, remote attackers to take over infrastructure or gain access to internal networks through exploitation of vulnerable internet-facing systems or interfaces. A dozen of 2021's widespread threat CVEs require chaining with additional vulnerabilities for successful exploitation; the ProxyLogon and ProxyShell attacks against Microsoft Exchange Server are the best-known examples of this, but they're not alone.

Seventeen of 2021's broadly exploited CVEs—more than half of the year's widespread threats—were under attack before patches were available, in comparison with arguably only one of the widespread threats from 2020. While we considered three of 2020's widespread threats to be zero-day vulnerabilities, arguably only one of them was probably a zero-day exploit used in the wild by adversaries. That zero-day, CVE-2020-14750, was a patch bypass for CVE-2020-14882 which saw widespread exploitation in late 2020. The remaining flaws (CVE-2020-10189 and CVE-2020-17496) fell into the zero-day vulnerability category because the researchers who discovered them released exploit code prior to patch availability. But a researcher is not an adversary—and public proof-of-concept code is not the same as an in-the-wild attack.

The ProxyLogon vulnerabilities in Microsoft Exchange Server account for nearly a third of 2021 zero-day exploits, but they have plenty of company—Pulse Connect Secure, Accellion FTA, SonicWall SMA 100 series, QNAP NAS, Windows Print Spooler, Apache HTTP Server, and Log4Shell all make notable entries in this category.

Several media outlets and research groups have written about 2021's record-setting zero-day count, but client-side and host-based vulnerabilities tend to be more represented in well-known datasets of zero-day exploits used in the wild (most notably Google Project Zero's "0day In the Wild" series) than server-side CVEs.

Because Rapid7's vulnerability research and emergent threat response teams focus on the vulnerabilities likeliest to be exploited at scale over a significant period of time, we generally leave browser and host-based zero-day bugs out of scope, with a few rare exceptions. Our emphasis on server-side vulnerabilities rather than client-side flaws means the number of zero-day CVEs in our dataset actually *underrepresents* the true volume of zero-day exploitation detected in 2021.

Other Known Exploited Vulnerabilities

CVE	Threat Status	Attacker Utiliity	Vulnerability Class	Time to Known Exploitation (TTKE) in Days
CVE-2020-7961 Liferay Portal Unauthenticated Remote Code Execution	• Exploited in the wild	Remote code execution	Deserialization	Unknown
CVE-2021-21307 Lucee Administrator Unauthenticated Remote Code Execution	• Exploited in the wild	Remote code execution	Improper Access Control	Unknown
CVE-2021-1732 Microsoft Windows Win32k Elevation of Privilege	• Exploited in the wild (0day)	Local code execution	Memory Corruption	0
CVE-2021-21975 VMware vRealize Operations Manager API Server-Side Request Forgery	• Exploited in the wild	Network infrastructure compromise	Improper Access Control	Unknown
CVE-2021-30657 Apple macOS Gatekeeper Bypass	• Exploited in the wild (0day)	Local code execution	Improper Access Control	0
CVE-2021-21551 Dell dbutil Driver Insufficient Access Control	• Exploited in the wild	Local code execution	Improper Access Control	13
CVE-2021-1497 Cisco Hyperflex HX Command Injection	• Exploited in the wild	Network infrastructure compromise	Injection / Command	31
CVE-2021-36934 Microsoft Windows Elevation of Privilege "Serious SAM"	• Exploited in the wild	Local code execution	Improper Access Control	Unknown

CVE	Threat Status	Attacker Utiliity	Vulnerability Class	Time to Known Exploitation (TTKE) in Days
CVE-2021-40539 Zoho ManageEngine ADSelfService Plus Authentication Bypass	• Exploited in the wild (0day)	Remote code execution	Improper Access Control	0
CVE-2021-40438 Apache HTTP Server Server-Side Request Forgery	• Exploited in the wild	Network infrastructure compromise	Injection / SSRF	69

2021's crop of regular old exploited-in-the-wild vulnerabilities includes a few lesser-seen targets than the widespread threat group, as well as more diversity in attacker use cases. MacOS, Dell driver, and Windows kernel flaws add some local execution representation to this category. CVE-2021-1732, a local privilege escalation bug in Win32k, provided new opportunities for arbitrary reads in Windows kernel memory—a fresh exploitation primitive for attackers. Apache HTTP Server CVE-2021-40438 made fewer waves than some other bugs when it was first disclosed, despite the fact that it was exploited quickly. Because other vendors bundle HTTP Server in their products, we expect CVE-2021-40438 to have a long tail.

Rapid7 managed services teams observed exploitation of CVE-2021-21307, an unauthenticated RCE vulnerability in Lucee Administrator, several months after security researchers released details on its place in an exploit chain they used to hack Apple. Multiple security companies reported exploitation of Liferay Portal CVE-2020-7961 in January 2021, more than a year after the vulnerability was publicly disclosed; notably, a Metasploit module has been available for CVE-2020-7961 since April 2020. VMware vRealize Operations Manager (CVE-2021-21975) joined CISA's Known Exploited Vulnerabilities in January 2022 along with vRealize Operations Manager CVE-2021-21983—together, the two vulnerabilities form a remote code execution chain.

Because so many zero-day attacks migrated to the widespread threat category in 2021, only 30% of the CVEs in this group were the result of pre-patch zero-day exploits, versus about half in 2020. While none of these vulnerabilities are known to be widely exploited at time of writing, the general uptick in at-scale attacks means that we can no longer call known-exploited vulnerabilities "targeted" threats with high confidence. It's more accurate to simply note that we do not yet see evidence of widespread exploitation.

In the past, the targeted threats we've analyzed have shared certain characteristics: Zero-day exploitation is commonplace, and memory corruption tends to be overrepresented as a root cause—a favorite vulnerability class for APTs and sophisticated threat actors thanks to the deep access it provides. Most importantly, almost all of the vulnerabilities in our 2020 list of targeted threats were reported as exploited in the wild by only a single data source. This is rarely the case anymore, in part because detection and tracking have improved, but also because even advanced attackers are using ransomware—which relies on volume for profitability—in their operations.

SolarWinds Serv-U CVE-2021-35211 illustrates this point perfectly: It's a model memory corruption zero-day that carried the much-maligned "limited and targeted exploitation" caveat when it was disclosed in July 2021. Those characteristics are usually a sign that broader exploitation is unlikely; many memory corruptions are difficult to develop attacks for and tend toward instability (though when exploitation is successful, it can give attackers the ability to execute arbitrary code in memory space). Despite its textbook "limited and targeted" use case, security researchers observed a threat actor leveraging CVE-2021-35211 as an initial access vector for Clop ransomware in November 2021, which moved it out of the mere "known exploited" category and into our collection of widespread threats.

Impending Threats

CVE	Threat Status	Attacker Utiliity	Vulnerability Class
CVE-2020-25223 Sophos UTM Remote Code Execution	• **Impending - Exploit available**	Network pivot	Injection / Command
CVE-2021-26914 NetMotion Mobility Arbitrary Code Execution	• **Impending - Exploit available**	Network pivot infrastructure compromise	Deserialization
CVE-2020-7388 Sage X3 ERP Remote Code Execution	• **Impending - Exploit available**	Remote code execution infrastructure compromise	Improper Access Control
CVE-2021-34481 Microsoft Windows Print Spooler Remote Code Execution	• **Impending - Exploit available**	Remote code execution	Injection
CVE-2021-2394 Oracle WebLogic Server Remote Code Execution	• **Impending -** High-value target	Remote code execution	Deserialization
No CVE Microsoft Azure Cosmos DB Unauthorized Privileged Access "ChaosDB"	• **Impending -** High-value target	Network infrastructure compromise	Improper Access Control
CVE-2021-43287 GoCD Pre-Authenticated Build Pipeline Takeover	• **Impending -** High-value target	Information disclosure	Improper Access Control

Rapid7's 2020 vulnerability intelligence report examined 20 impending threats that we considered high-value targets for attackers; since that report was released in Q1 2020, five of those vulnerabilities have become known active threats, with three seeing widespread exploitation (CVE-2020-2021, CVE-2020-5135, and CVE-2020-16846). The number of impending threats in our 2021 dataset has dwindled, in part, because vulnerabilities that our teams analyzed have come under attack more quickly than in previous years. Cisco Hyperflex CVE-2021-1497, VMware vRealize Operations Manager CVE-2021-21975, and Microsoft Windows CVE-2021-36934 are among the vulnerabilities that were impending threats when we first analyzed them but were exploited in the wild by the time we finalized our 2021 data.

Still, there are a few CVEs that stand out for their exploitability and/or the value they offer attackers. It's difficult to imagine that adversaries have yet to weaponize CVE-2021-2394, a trivially exploitable deserialization flaw in Oracle WebLogic Server—a popular target that got an unexpected reprieve in 2021. Likewise, remote code execution in Sage X3 productivity software (CVE-2020-7388) and network pivot vulnerabilities in Sophos Unified Threat Management (CVE-2020-25223) and NetMotion Mobility (CVE-2021-26914) solutions provide tempting initial access vectors for remote attackers.

A couple of the CVEs we've highlighted in this category are interesting Microsoft vulnerabilities: **CVE-2021-34881** is a remote code execution bug in the ever-exploitable Windows Print Spooler, the end product of two features intended to make the (non-administrative) user's life easier, and "**ChaosDB**" is a nifty little unauthorized access vulnerability in Azure's flagship CosmosDB (sans CVE). Last but not least, in a nod to the security world's sharpening focus on supply chain risk, our research team took a closer look at **CVE-2021-43287**, a pre-authentication information disclosure vulnerability in GoCD, an open-source CI/CD server.

We recommend prioritizing patch installation for these vulnerabilities. The "exploit available" references in this table all represent Metasploit modules that have been developed and tested for compatibility across a range of platforms. Metasploit is not the only toolkit we consider to be mature as far as attacker capabilities go, but we have high confidence in the efficacy of the exploit code our own researchers have developed and tested for these CVEs.

We recommend prioritizing patch installation for these vulnerabilities.

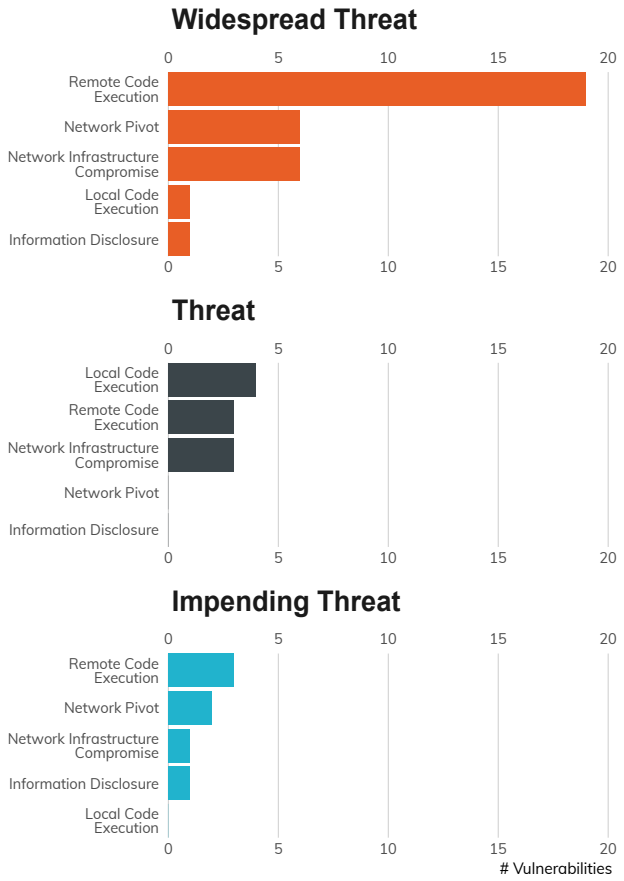
2021 Attack Trends

Attacker Utilities and Vulnerability Classes

When getting to know a new vulnerability, the first thing our research teams look for is an understanding of the root cause and what an attacker might use that bug to achieve. Vulnerabilities arise from hundreds of conditions spanning all layers of the stack—from application programming errors to cryptographic implementations to hardware bugs. Likewise, the potential impact of any given vulnerability can vary widely based on implementation, security controls, and the sensitivity of the data or permissions an attacker can obtain as a result of exploitation.

We include two additional types of metadata in our 2021 vulnerability data in addition to threat status and time to known exploitation. The first type of metadata our researchers define when analyzing emergent threats is **attacker utility**, which describes what an attacker can hope to gain as a result of successful exploitation and often maps to part of an exploit chain.

2021 Vulnerabilities by Attacker Utility and Threat Status



Much like in 2020, vulnerabilities that provided attackers with remote code execution opportunities—the ability to remotely execute a payload on a target system—are the most represented type of attacker utility across the 50 CVEs in this report, at just over half of the total dataset. Remote code execution is how vendors and CVE numbering authorities (CNAs) frequently describe high-impact vulnerabilities, but in some cases, that description downplays the ways that severe CVEs can be used to further compromise a network. A dozen of 2021's widespread threats, for instance, were CVEs that we categorized as either **network pivots** or **network infrastructure compromise** vulnerabilities.

Network pivots, also known as initial access vectors, are vulnerabilities that give external attackers internal (authenticated) network access, allowing them to move laterally, escalate privileges, and exploit systems that wouldn't otherwise be accessible to them. Vulnerabilities in security boundary devices like VPNs, firewalls, and gateways are high-value network pivot opportunities for both sophisticated and low-skilled adversaries, as are vulns in management interfaces and exposed services that can be exploited for network access. SonicWall SMA 100 series CVE-2021-20016, F5 iControl REST CVE-2021-22986, and Pulse Connect Secure CVE-2021-22893 are all examples of network pivot opportunities arising from traditional security gateway technologies. Backdoor administrative access vulnerabilities in QNAP network-attached storage (CVE-2021-28799) and SonicWall Email Security (CVE-2021-20021) solutions also contributed to the widespread attack list in 2021.

Network infrastructure compromise vulnerabilities are flaws residing in systems that, when exploited successfully, give attackers the ability to compromise downstream (networked) systems and services. Vulnerabilities in virtualization, automation, and device management infrastructure all fall into this category. 2021's network infrastructure compromise flaws included three high-severity vulnerabilities in vCenter Server, plus the first CVE in an attack chain against VMware's vRealize Operations Manager product (CVE-2021-21975). A command injection vuln in Cisco Hyperflex HX (CVE-2021-1497, another chain) and an unauthorized access bug in Azure's Cosmos DB made for other interesting entries in this category.

Local code execution was less prevalent among significant threats in 2021, which is hardly surprising since it's much easier to launch internet-scale attacks from, well, the internet. Still, CVE-2021-30657, a nifty security feature bypass in macOS, bears mentioning. Information disclosure similarly tends to be underrepresented among active, high-profile threats, but it probably shouldn't be—info leaks are incredibly helpful to savvy adversaries when developing multi-step attacks, as long-running threat campaigns have proven time and again (see CVE-2018-13379 and CVE-2019-11510). In 2021, Kaseya VSA's zero-day credential disclosure gave rise to the REvil ransomware outbreak that ruined MSPs' Fourth of July weekends, and "SeriousSAM" paved a clear path to SYSTEM-level access in Windows environments.

We've also defined four intentionally broad vulnerability classes that are useful for making initial assessments about relative exploitability and available attacker tooling: improper access control, memory corruption, injection, and deserialization.

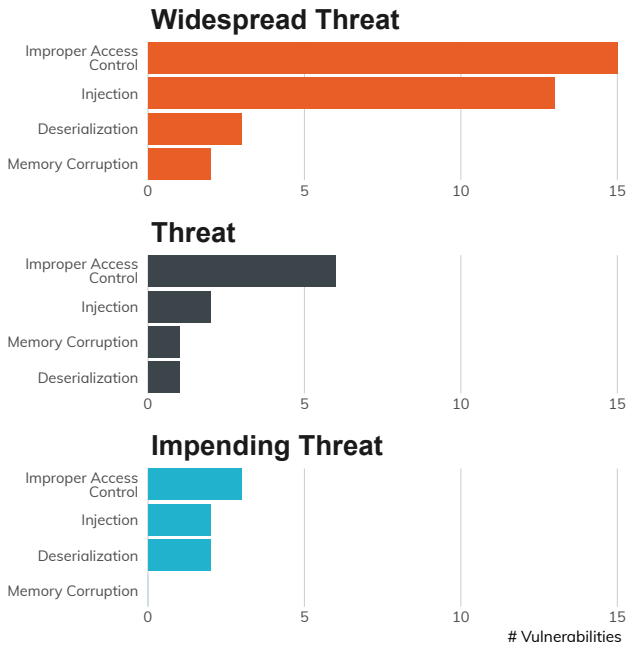
Deserialization vulnerabilities come with a reputation for high exploitability and have a wealth of off-the-shelf tools with which to build exploit chains. Memory corruption vulnerabilities make frequent appearances in attacks by sophisticated threat actors; they offer privileged access and stealth, but are difficult to develop, unlikely to be automated, and tend toward instability—all of which make them good for targeted attacks but unreliable for more widespread exploitation. Improper access control flaws typically indicate something is missing (like an authentication requirement) or configured to be permissive, which allows attackers access that might otherwise be gated by security controls. And injection attacks use specially crafted input and techniques to compromise data integrity or run arbitrary code as a high-privileged user.

Vulnerability class is an umbrella term that encompasses both root cause and the type of high-level technique that might trigger it. As a result, some of our vulnerability class categorizations might seem unusual. For example, we classify certain file upload, file write, and server-side request forgery vulns as injection flaws in addition to more traditional command and SQL injection vulnerabilities—indexing on the type of technique an attacker must use to exploit those vulnerabilities.

There was a huge increase in attacks that used injection techniques in 2021, including for widely exploited vulnerabilities. Injection attacks use specially crafted input and techniques (e.g., SQL injection, command injection, JNDI injection, OGNL injection) to compromise data integrity or run arbitrary code as a high-privileged user.

These attacks tend to be stable and reliable, which makes them less likely to knock over systems than, say, attacks leveraging memory corruption flaws. The most infamous of 2021's injection vulns is Log4Shell, the JNDI injection flaw in open-source Java logging library Log4j that set the internet aflame in December 2021, but it wasn't the first JNDI injection bug to make waves in 2021—vCenter Server CVE-2021-21985 preceded it by more than six months. OGNL injection in Confluence Server (CVE-2021-26084), SQL injection in Accellion FTA appliances (CVE-2021-27101), and vanilla command injection in Cisco, F5, and Sophos products make up some more of 2021's malicious request volume.

2021 Vulnerabilities by Class and Threat Status



A Little Goes a Long Way: Server-Side Request Forgery

While we're on the topic of malicious requests and injection attacks, server-side request forgery (SSRF) vulnerabilities featured prominently in several of 2021's high-impact attack campaigns. SSRF is a powerful technique that allows an attacker to send arbitrary requests that cross security boundaries or internal product boundaries. Depending on the vulnerability and its location in the target tech stack, those arbitrary requests may leak credentials, exploit a hidden endpoint, or fetch resources the attacker would not otherwise be able to access.

For the first time in 2021, SSRF made OWASP's top 10 application security risks, claiming the final spot on the list based on community survey results.

SSRF's commonality nowadays arises in part because of the explosion of complex, layered applications that comprise significant portions of organizations' public-facing attack surface area. Web applications are a critical starting point for many attacks that end in remote code execution or remote access; classic SSRF lets an external attacker submit a crafted request (such as a malicious GET or POST request) to an application's front end and coerce the back-end server into doing something that aids the attacker's operations, like authenticating to the domain or forwarding requests to arbitrary servers—making SSRF an ideal first step for attack chains.

Several of those chains became widespread threats in 2021. The ProxyLogon chain of vulnerabilities begins with CVE-2021-26855, a server-side request forgery flaw that allows an attacker to send arbitrary HTTP requests and authenticate as the Exchange server. When chained with additional ProxyLogon CVEs, the SSRF leads to unauthenticated, SYSTEM-level remote code execution on vulnerable targets. The first CVE in the ProxyShell exploit chain (CVE-2021-34473) works similarly, though it's not technically classified as SSRF. Orange Tsai, the researcher who discovered both chains, described the SSRF-like technique that kicks off ProxyShell exploitation:

> **"It too appears when the frontend (known as Client Access Services, or CAS) is calculating the backend URL. When a client HTTP request is categorized as an Explicit Logon Request, Exchange will normalize the request URL and remove the mailbox address part before routing the request to the backend."**

An SSRF vulnerability in Accellion FTA devices (CVE-2021-27103) linked with a command execution vulnerability (CVE-2021-27102) made up one of the two attack chains that compromised Accellion customers using the company's legacy File Transfer Appliance in early 2021. A forensic investigation into the incident revealed a new type of webshell that cybersecurity firm Mandiant christened "DEWMODE." Later in the year, CVE-2021-40438 allowed remote, unauthenticated attackers to force vulnerable Apache HTTP servers using `mod_proxy` to forward requests to arbitrary (malicious) servers; Rapid7 Labs observed four million potentially vulnerable httpd instances on the public internet in September 2021, even without accounting for all the critical downstream solutions that bundle Apache web servers.

Finally, Rapid7 researchers analyzed and demonstrated exploitability for CVE-2021-21975, a server-side request forgery vulnerability in VMware's vRealize Operations Manager solution, in March 2021. It was added to CISA's Known Exploited Vulnerabilities list in January 2022.

OWASP's page on SSRF in 2021 includes a statement worth highlighting: "The data shows a relatively low incidence rate with above average testing coverage and above-average Exploit and Impact potential ratings." Despite the severity of some of 2021's SSRF-driven attack chains, there's likely an element of self-fulfilling prophecy in community assessments about the technique's overall importance. It's an easy weakness to test for so long as the tester can find a field that accepts a URL, which makes it popular with bug bounty hunters in addition to real adversaries. It's a beginner-friendly technique that presents internet-facing surface area, so it's no surprise that the community has found a lot of it.

Attack Chains

As the architecture of software and systems grows ever more complex, attack complexity continues to increase, too. The vulnerabilities we've highlighted from 2021 include 16 CVEs across 11 unique attack chains, many of which we have already discussed and each of which requires linking multiple vulnerabilities for successful exploitation.

ProxyLogon (four CVEs) and ProxyShell (three CVEs) comprise almost half of chained vulnerabilities in our dataset but only represent two of the unique chains. The following vulnerabilities make up some additional 2021 attack chains, several of which have one or more sibling CVEs not included in this report.

CVE	Threat Status	Attacker Utiliity	Vulnerability Class	Exploit Chain
CVE-2020-7388 Sage X3 ERP Remote Code Execution	• **Impending - Exploit available**	Remote code execution	Improper Access Control	CVE-2020-7387, CVE-2020-7389
CVE-2021-43287 GoCD Pre-Authenticated Build Pipeline Takeover	• **Impending** - High-value target	Information disclosure	Improper Access Control	Exploit Primitive (GoCD)
No CVE Microsoft Azure Cosmos DB Unauthorized Privileged Access "ChaosDB"	• **Impending** - High-value target	Network infrastructure compromise	Improper Access Control	Exploit Primitive (Microsoft Azure)
CVE-2021-21975 VMware vRealize Operations Manager API Server-Side Request Forgery	• **Exploited in the wild**	Network infrastructure compromise	Improper Access Control	CVE-2021-21983
CVE-2021-36942 Microsoft Windows LSA Spoofing "PetitPotam Attack"	• **Widespread Threat**	Network infrastructure compromise	Improper Access Control	AD CS
CVE-2021-34523 Microsoft Exchange Server Elevation of Privilege "ProxyShell"	• **Widespread Threat**	Local code execution	Improper Access Control	ProxyShell
CVE-2021-34473 Microsoft Exchange Server Remote Code Execution "ProxyShell"	• **Widespread Threat**	Remote code execution	Improper Access Control	ProxyShell
CVE-2021-31207 Microsoft Exchange Server Security Feature Bypass "ProxyShell"	• **Widespread Threat**	Remote code execution	Injection / Request	ProxyShell

CVE	Threat Status	Attacker Utility	Vulnerability Class	Exploit Chain
CVE-2021-27101 Accellion FTA Unauthenticated SQL Injection	• **Widespread Threat** (0day)	Remote code execution	Injection / SQL	CVE-2021-27104
CVE-2021-27103 Accellion FTA Server-Side Request Forgery	• **Widespread Threat** (0day)	Remote code execution	Injection / Request	CVE-2021-27102
CVE-2021-26857 Microsoft Exchange Server Unified Messaging Deserialization "ProxyLogon"	• **Widespread Threat** (0day)	Remote code execution	Deserialization	ProxyLogon
CVE-2021-26858 Microsoft Exchange Server Arbitrary File Write "ProxyLogon"	• **Widespread Threat** (0day)	Remote code execution	Injection / File	ProxyLogon
CVE-2021-27065 Microsoft Exchange Server Arbitrary File Write "ProxyLogon"	• **Widespread Threat** (0day)	Remote code execution	Injection / File	ProxyLogon
CVE-2021-26855 Microsoft Exchange Server-Side Request Forgery "ProxyLogon"	• **Widespread Threat** (0day)	Remote code execution	Injection / Request	ProxyLogon
CVE-2021-30116 Kaseya VSA Credential Disclosure	• **Widespread Threat** (0day)	Information disclosure	Improper Access Control	Exploit Primitive (Kaseya VSA)
CVE-2021-20021 SonicWall Email Security Pre-Authentication Administrative Account Creation	• **Widespread Threat** (0day)	Network pivot	Improper Access Control	Exploit Primitive (SonicWall Email Security)

In general higher attack complexity offers some benefit for software producers tasked with developing mitigations, but it also presents advantages for attackers. Vulnerability and exploit complexity can make it difficult for software developers to create corresponding solutions quickly and effectively, which in some cases means vendors implement security fixes that merely add filtering to one part of the attack chain rather than more comprehensively addressing the root cause. This isn't necessarily ineffective as a fast, narrowly tailored solution for users, but it can also leave attackers clear opportunities to bypass filters (e.g., authentication).

Bring Your Own Vulnerable Driver (BYOVD)

There's been a resurgence of driver-based attacks the past few years, with several high-profile 2021 vulnerabilities illustrating the utility of "Bring Your Own Driver" (BYOVD)-style exploits. In this type of attack, an adversary with administrative privileges installs a legitimately signed driver with known vulnerabilities on the victim system—which is where product security incident response teams (PSIRTs) tend to lose interest when evaluating a BYOVD vulnerability disclosure, since administrator-level privileges are required from the get-go.

For those unfamiliar with BYOVD attacks, the number one reason adversaries are using BYOVD is to bypass Windows Driver Signature Enforcement (DSE), which ensures that only signed kernel drivers can be loaded. By installing and exploiting a vulnerable driver, attackers can load their own unsigned malicious drivers, which allows them to accomplish a wide variety of tasks they wouldn't be able to otherwise (e.g., unhooking EDR callbacks, hiding exploitation/rootkit artifacts, overwriting data, injecting code into other processes).

Most of the attacks mentioned above focus on executing code in kernel mode. But BYOVD also enables a simpler data-oriented attack that allows an adversary to subvert Local Security Authority (LSA) protection. LSA protection prevents non-protected processes from reading the memory of, or injecting code into, Windows' Local Security Authority Subsystem Service (lsass.exe). That means tools like Mimikatz can't dump the memory contents of `lsass.exe` in order to retrieve Windows account credentials. An attacker with kernel-mode access—also known as ring 0 access—can reach into the `lsass.exe` EPROCESS struct and simply mask out the LSA protection, leaving the attacker free to dump `lsass.exe`'s memory. There are a couple of good open-source implementations of this: mimidrv (a signed driver that is part of Mimikatz) and PPLKiller (uses RTCore64.sys).

In December 2021, Rapid7's vulnerability research team compiled a list of several dozen well-known driver-based attacks, including CVEs, driver names, and adversary attribution where available. While the catalog our team compiled isn't necessarily exhaustive, there have been more prominent driver-based attacks in 2020 and 2021 than in the prior eight years combined. Our 2021 vulnerability intelligence dataset highlights two CVEs that enable BYOVD attacks: CVE-2021-21551, a local privilege escalation in Dell's dbutil_2_3.sys driver that has reportedly been exploited in the wild; and CVE-2021-34481, which makes yet another remote code execution vulnerability in the Windows Print Spooler.

CVE-2021-34881 is the combination of two features intended to make non-administrative Windows users' lives easier by expansively allowing them to add remote printers and also to add arbitrary *signed* drivers to the driver store… before installing them at will. As a result, low-privileged users could install a vulnerable print driver and exploit it to gain `SYSTEM` privileges. CVE-2021-21551 arises from a write-what-where condition (CWE-123) in which a low privileged user can direct the driver to write attacker-controlled data to an arbitrary memory address via an ioctl call. This allows low-privileged users to escalate permissions to `SYSTEM` by overwriting data structures in kernel memory.

Since network-based intrusion detection systems aren't good options for identifying local exploitation of vulnerable drivers, the best approach for defenders may be intentionally, if arduously, limiting attack surface area. CVE-2020-17382, for example, targeted a driver that controlled the RGB lights on gaming motherboards, making it the type of driver that (just maybe!) could sensibly be left out of enterprise builds. Microsoft also maintains a list of driver block rules that, if used correctly, will allow systems administrators to block known-bad drivers from being loaded. The Dell drivers, which are used to update firmware across a wide range of products, are compatible with the newest signing requirements issued by Microsoft and admittedly have a low likelihood of being blocklisted, though we remain eternally optimistic.

Finally, it's worth noting that BYOVD attacks present a slight conundrum for security researchers, and therefore to downstream practitioners and organizations who benefit from good-faith security research artifacts like public proof-of-concept code. Because step zero of a BYOVD attack is installing a third-party driver (hence the "Bring Your Own"), researchers and their employers must consider the risk of potentially violating licensing agreements—a provision that stops ethical hackers from easily sharing exploit code or other tooling with defenders, but has no effect whatsoever on adversaries who conduct driver-based attacks in the wild without compunction.

"

there have been more prominent driver-based attacks in 2020 and 2021 than in the prior eight years combined.

Chain Reaction: Present and Future Software Supply Chain Risk

Unsurprisingly, the discovery of a backdoor in SolarWinds Orion set off waves of global concern about supply chain security writ large, from software development pipelines and CI/CD tooling to shared libraries and upstream service providers. Even tangentially supply chain-related compromises have engendered high alarm, with traditional product zero-day attacks like the Accellion FTA incident being likened to the SolarWinds compromise. In other words, supply chain anxiety was always here, but the SolarWinds incident kicked it into higher gear.

The risk wasn't theoretical, either. In the first half of 2021, PHP's Git repository was hacked and a backdoor added to PHP source code via several malicious commits made by legitimate committer accounts, one of which belonged to PHP's creator. Fortunately, the malicious code was identified quickly and never made it into production; nevertheless, the incident prompted PHP's maintainers to abandon their self-maintained infrastructure and lock down their development workflows. Alas, other incidents had farther-reaching effects. In April, code quality tool Codecov announced that a threat actor had gained access to Codecov's popular Bash Uploader script and modified it to allow the export of continuous integration (CI) environment secrets, including credentials, tokens, and keys. The threat actors had gained access to the Bash Uploader in January 2021—more than three months before Codecov detected and disclosed the hack.

Vulnerabilities in shared libraries and common components also posed a threat in 2021, even before Log4Shell arrived to underscore the pain of detecting and remediating deeply embedded flaws. The last quarter of the year bore witness to not one, but three separate hijacks of wildly popular NPM libraries: In October, multiple versions of the UAparser.js JavaScript library were modified to install coin miners and harvest credentials on downstream systems, drawing a warning from GitHub that any computer with the package installed or running should be considered fully compromised. A little over a week later, two additional NPM packages—`coa` (Command-Option-Argument) and `rc`—were found to have shipped to downstream developers with embedded malware. On November 15, 2021, even as it disclosed another high-severity security vulnerability in the NPM registry, GitHub announced that NPM package maintainers and administrators would be required to implement two-factor authentication (2FA) starting in 2022.

Devops tooling and software packages will logically remain high-value targets for both sophisticated and opportunistic adversaries. One of the vulnerabilities that piqued our team's interest last year was CVE-2021-43287, an unauthenticated information disclosure in open-source CI/CD server GoCD that was exploitable with a single HTTP request and allows for pre-authentication takeover of CI/CD pipelines. While CVE-2021-43287 is in our impending threat category—not known to be exploited in the wild at time of writing—it's the type of flaw we expect to garner closer scrutiny from the research community, and from attackers, in 2022.

Managed service providers (MSPs) and managed security service providers (MSSPs) have also been key attack targets for threat actors looking for access to downstream customers and environments. In early July 2021, just as the long Independence Day weekend kicked off in the U.S, managed service provider Kaseya VSA unwittingly pushed out a malicious automatic update containing REvil ransomware to some on-premise customers. In the hours that followed, Kaseya shut down its SaaS servers and advised customers around the world to shut down their on-premise VSA servers. The initial access vector, it transpired, was CVE-2021-30116, a zero-day credential disclosure vulnerability in Kaseya VSA that had been reported to Kaseya in April 2021 by the Dutch Institute for Vulnerability Disclosure (DIVD) along with half a dozen other vulnerabilities.

On the subtler end of the attack spectrum, Microsoft warned the public in October 2021 that Russian state-sponsored threat actor Nobelium was targeting the global technology supply chain, in particular resellers, managed service providers, and cloud service providers (CSPs). According to Redmond, more than a dozen resellers and service providers had been identified as potentially compromised by threat activity aimed at gaining long-term access to the IT supply chain.

It's common sense to expect this will continue. Initiatives like Software Bill of Materials (SBOM) requirements aim to make it simpler for software developers, users, and stakeholders to understand the components and dependencies bundled into the technologies they rely upon. As Rapid7 researchers have previously discussed, however, the continuing global shift to fully cloud-based applications complicates the development of comprehensive SBOMs. Cloud misconfigurations have also become an increasingly prevalent source of vulnerabilities across the SaaS ecosystem, multiplying potential points of risk. Information and intelligence sharing will continue to be important parts of preventative defense against supply chain attacks as broader policies and practices evolve toward greater transparency and security.

Spotlight: Key 2021 Windows Vulnerabilities

Evacuate the (On) Premises: We Need to Talk About Exchange

One unusually balmy Saturday in February of 2021, Rapid7's Managed Detection and Response team noticed an increase in alerts firing on known attacker behavior. Their systems were picking up a sudden spike in exploitation of on-premise Microsoft Exchange servers whose web services were exposed to the public internet—a common practice for organizations that rely on Outlook Web Access (OWA) for email. The exploits aimed at Exchange were uploading `eval` webshells, colloquially referred to as "Chopper" or "China Chopper" webshells. Over the next few days, our SOC and incident response teams investigated attacker activity across dozens of customers—a flurry of activity that, as it turned out, was being mirrored in security operations centers around the world as incident responders and analysts tried to determine what was causing such an abrupt wave of compromises.

The afternoon of March 2, 2021, three days after the rash of attacks had begun, Microsoft released an out-of-band security advisory and accompanying analysis on four zero-day vulnerabilities in on-premise Exchange Server installations that were being targeted by a state-sponsored threat actor Microsoft's Threat Intelligence Center dubbed "HAFNIUM." The zero-day vulnerabilities—comprising a server-side request forgery (SSRF) bug, a deserialization flaw, and two post-authentication arbitrary file writes—together allowed attackers to access email, install additional malware, and establish persistence in victim environments via an exploit chain called "ProxyLogon" that would wreak havoc on Exchange instances for months following the out-of-band disclosure.

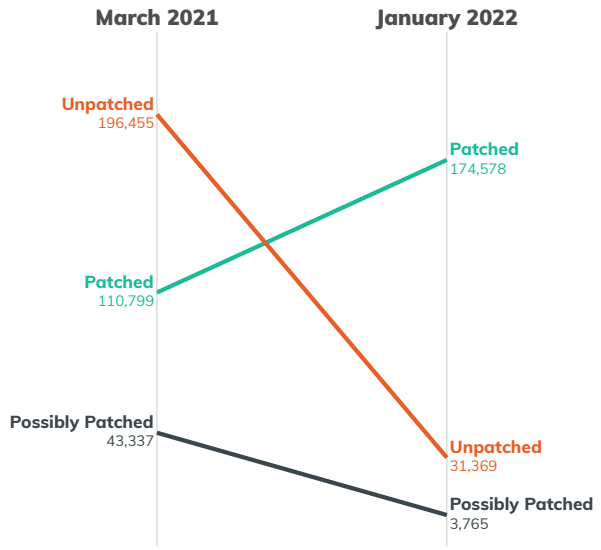
ProxyLogon presaged a particularly bad year for on-premise Exchange Server—or perhaps more accurately, represented an escalation in a multi-year arc of widespread attacks targeting severe Exchange Server CVEs. A Black Hat USA presentation by prominent researcher Orange Tsai in August 2021 revealed a second critical exploit chain against on-premise Exchange called "ProxyShell" which, though it saw no pre-disclosure exploitation, was used in the wild by adversaries starting barely a week after its Black Hat debut. By the end of August, opportunistic attackers (including ransomware operators) had compromised hundreds of Exchange Server environments using ProxyShell, and security community discussions were full of debates on the practicality and cost-effectiveness of moving away from on-premise Exchange use post haste.

In addition to the seven Exchange vulnerabilities collectively included in the ProxyLogon and ProxyShell chains, at least three other Microsoft Exchange Server CVEs were used in the wild in 2021 (CVE-2021-42321, a zero-day vulnerability from November's Patch Tuesday; CVE-2021-28480, an NSA-reported flaw that researcher Kevin Beaumont detected in the wild in May; and CVE-2021-33766, an information disclosure). Despite this, Exchange Server vulnerabilities continue to offer a target-rich environment for attackers. Each new Exchange RCE—whether exploit chain or standalone vulnerability—seems to bring with it a wave of fresh compromises, no matter how many dire warnings populate email alerts and internet headlines.

Exchange Patching: How it Started / How It's Going

2021 was a wild ride for folks running Microsoft Exchange

We saw thousands fewer Exchange servers on the internet by the end of the year, and over all improved patching for the ones that remained connected to the internet.



In March, Rapid7 Labs observed a migration of Exchange Server instances off the public internet, as ProxyLogon laid waste to Windows environments worldwide. Throughout 2021, vulnerable Exchange Server installations dwindled across public exposure maps—indicating that administrators understood the attack surface area they had been offering remote adversaries, and that they had moved to limit it. But the compromises kept coming: Why? The simplest answer is that many Exchange admins took their vulnerable instances off the internet but either couldn't or wouldn't patch their servers despite sustained threat campaigns.

A likelier explanation is that the call was already coming from inside the building—even for non-zero-day Exchange CVEs, the pace of exploitation has been so rapid that defenders may not have had sufficient time to remediate new vulnerabilities before adversaries made it into their networks.

In Rapid7's **2020 Vulnerability Intelligence Report**, we said we considered most critical-rated and many important-rated in Microsoft Exchange and SharePoint to be strong impending threat candidates regardless of whether exploit code has been released. Since February 2020, our emergent threat response team has initiated urgent responses for nine Microsoft Exchange Server vulnerabilities. By the end of summer's hacker conference season in the U.S., ransomware groups had efficiently **incorporated** ProxyShell into their operations along with ProxyLogon, prompting renewed calls for organizations to move off of on-premise Exchange from the security community. The reality for most security teams, however, is that security is a negotiation, and a wholesale move to the cloud isn't an option that's within reach for many companies.

In the meantime, Exchange administrators and IT teams should remember that limiting exposure is important, but it's not enough on its own. Patching is still a critical, time-sensitive step.

Nightmares and Novelties

A trio of named Windows vulnerabilities drove **confusion** and **consternation** over the summer of 2021, largely due to Microsoft's opaque vulnerability disclosure and information sharing practices. PrintNightmare (**CVE-2021-34527**), Serious SAM (**CVE-2021-36934**), and PetitPotam (**CVE-2021-36942**) threatened Windows environments over a three-week period starting in July—following what had already been a dizzying first half of the year that saw no fewer than two dozen emergent threats. Each flaw broke on Twitter, where proof-of-concept exploits and attack demos circulated freely hours and sometimes days before official acknowledgment and guidance came down from Redmond.

The Windows Print Spooler has been a cyclically popular target for both attackers and security researchers. The summer security conference season brought new critical CVEs in the service in 2020 and again in 2021, each of which was exploited in the wild **quickly**. Realistically, this probably isn't a surprise. Stuxnet may have been the most infamous attack to leverage a flaw in the Windows Print Spooler, but the service has a **long history** of flaws and—more importantly—enjoys a central, accessible place in many corporate networks.

When PrintNightmare (**CVE-2021-34527**) **hit the internet** in the last few days of June, the research community first thought that what they were exploiting was merely an incomplete fix for an earlier vulnerability in the Windows Print Spooler, **CVE-2021-1675**. (There was precedent for this: The patch for **CVE-2020-1048**, a critical Print Spooler RCE known as "PrintDemon '' that had received the **Black Hat treatment in 2020**, was bypassed at least twice before its fix was deemed successful.) By the time Microsoft issued an out-of-band advisory acknowledging the community's findings and a fresh zero-day CVE for the vulnerability that became known as "PrintNightmare," at least three distinct exploits had been shared in public code repositories and on social media.

Things got worse from there: Amid active attacks in the wild, Windows administrators were advised—including by Rapid7's emergent threat response team—to disable the print spooler service altogether pending a formal fix. The **fix** came on July 6 but was promptly declared incomplete by prominent community members, including Mimikatz maintainer **Benjamin Delpy** and CERT/CC's **Will Dormann**, both of whom demonstrated **exploits** against fully patched systems. Microsoft rejected those community findings, however; instead, they **blamed** continued PrintNightmare exploitability on **Point and Print**, a feature that allows users to create connections to remote printers and was enabled by default **until August 2021**. The (default) Point and Print behavior, said Redmond, was an insecure setting that bypassed security boundaries. This was news to many organizations. Despite Microsoft's insistence that community reports of incomplete patches were incorrect, the damage to customer confidence had already been done.

Unofficial guidance emphasized the need to keep the print spooler service disabled anywhere it wasn't required, even after the PrintNightmare ostensibly ended. COVID may have briefly made printers a smaller part of day-to-day operations for some organizations, but by and large, making printing harder isn't a realistic option for many businesses. Alas, if history is a reliable guide, 2021's printer woes won't be the last we'll see.

Two additional Windows zero-day vulnerabilities appeared on social media in late July. On July 19, community researchers began **reporting** that the Security Account Manager (SAM) file on Windows 10 and 11 systems was **readable by all local users**. Within 24 hours, a proof-

of-concept exploit had been released, enabling non-admin users to escalate to SYSTEM. Microsoft issued CVE-2021-36934 for the vulnerability, which had been christened "SeriousSAM" and "HiveNightmare." Despite the ongoing community attention, a patch wasn't available until August 10—not unprecedented as far as patch lag times go, but difficult to stomach when so many Windows administrators were still in the middle of PrintNightmare remediation. When Rapid7 research teams compiled the data for this report, CVE-2021-36934 was categorized as an impending threat; at the time, we noted that though we had no proof of exploitation in the wild, it beggared belief to imagine that attackers had failed to make use of an operating system-level information disclosure zero-day that went unpatched for weeks. In February 2022, CISA added the CVE to their known exploited vulnerabilities list.

The final zero-day flaw once again highlighted the long-standing risk NTLM relay attacks pose to Windows environments. Published to GitHub on July 18 by French security researcher Gilles Lionel, the "PetitPotam" exploit—named for a character in a French children's book series—implemented a classic forced authentication, Net-NTLM hash leak to a malicious third party. But PetitPotam stood out from its more run-of-the-mill cousins when the research community combined the exploit with elements of SpecterOps' "Certified Pre-Owned" attack chain. Using PetitPotam to leak a domain controller's computer account NTLM hash, a remote, unauthenticated attacker could relay the hash to an Active Directory Certificate Service (AD CS) to completely take over a Windows domain.

PetitPotam abuses Microsoft's MS-EFSRPC (Encrypting File System Remote Protocol) to trick a Windows host into authenticating to a malicious file share, resulting in the disclosure of the victim's machine account Net-NTLM hash. The attack is most powerful when used against a domain controller, but it can also be used against non-DC systems as well, as Rapid7 researchers confirmed (see "Testing Results"). Non-DC systems were also exploitable out of the box, but only when the attacker was authenticated (the authentication requirement no longer applied when the `lsarpc` named pipe was added to the server's allowlist for anonymous access). Exploitation of a non-DC machine account is heavily dependent on assigned permissions (e.g. assigned to the "Domain Admins" group); nevertheless, due to the lack of a complete patch for PetitPotam, the attack technique remains a viable path as of February 2022.

It took a few days for the full impact of the novel technique and its variants to permeate through the security community. It took longer for Microsoft to acknowledge the risk and release mitigation recommendations, which came five days after the PoC went public and confusingly—and incorrectly—emphasized the Active Directory Certificate Services use case rather than the attack's broader implications. Three weeks after PetitPotam first made waves and dismayed security teams, Microsoft issued CVE-2021-36942 in the August Patch Tuesday release alongside a note that the patch alone was not enough to protect affected systems. Five days later, on August 15, PetitPotam was updated to bypass the August patch anyway.

Windows administrators should disable SMBv1 in their environments and enable SMB signing. SMB signing prevents NTLM relay attacks like the one associated with PetitPotam.

We remind readers of these travails not to beat up on Microsoft, but rather to emphasize the importance of timely, accessible, actionable information sharing about the systems and services we rely upon so heavily. Large vendors have not been immune to the attrition and burnout challenges so many organizations faced in 2021; if anything, the effects of the cybersecurity talent shortage have been even farther-reaching when they emanate from large vendors like Microsoft. And finally, as attention-grabbing as PetitPotam may have been, several pen testers told us privately that novel relay attacks are usually unnecessary on their engagements—because older, even less complicated relay attacks still work just fine.

> **The Windows Print Spooler has been a cyclically popular target for both attackers and security researchers.**

Practical Guidance for Defenders

Despite patchy vendor guidance for some vulnerabilities in this report, the tried-and-true pieces of guidance in this section can afford defenders time and assist them in identifying suspicious or malicious activity. Though each security program—even those within the same organization—has different maturity and capability, these steps are battle-tested to make compromising organizations as hard as possible for attackers.

Rapid7 researchers publish analysis for high-priority vulnerabilities in Rapid7's community vulnerability assessment platform, AttackerKB. These analyses often include sample proof-of-concept code and indicators of compromise in addition to exploitation timelines and attack chain analysis. Those who wish to subscribe to notifications for formal Rapid7 analysis in AttackerKB can **create a free account**. Blogs on emergent threats are published **here**.

Get good at the basics of vulnerability management.

Robust **vulnerability management** is the foundation of any successful IT security program. Without the proactive discipline of vulnerability management and strong **routine patch management** practices developed during days of relative calm, it is nearly impossible to up-level to effective emergency patching in times of crisis. Incident response measures in the absence of proactive vulnerability management are also likely to be frenetic firefighting that is reactive and ineffective.

Within vulnerability management, asset inventory and patch management are foundational activities to get right. Good asset visibility is essential to many aspects of IT management. It's difficult to act quickly and decisively in a crisis if you don't know which technologies are present in your environment or where they live in your tech stack. Identify and catalog your critical and exposed systems, including security boundary devices, internet-facing load balancers, devops tooling and pipeline solutions, and virtualization infrastructure. For more fundamentals, read Rapid7's guidance on **security program basics**.

Limit and monitor your internet-facing attack surface area.

Understanding attack surface area and critical network entry points saves time when severe vulnerabilities surface in internet-facing technologies. Exploitation of many of the CVEs in this report—including some of those exploited in zero-day attacks—can be slowed down by limiting internet exposure of critical applications and management interfaces. Pay particular attention to security gateway products such as VPNs and firewalls, as well as anything else that's exposed by common practice or necessity. **CVE-2021-22893** and **CVE-2021-20016** are noteworthy examples.

Management and administrative interfaces should never be exposed to the public internet. The same goes for domain controllers and any other assets that organizations would not want an external attacker to be able to probe, such as IoT devices unwittingly exposed online. Audit internet-exposed attack surface area regularly, including via external penetration tests, if possible.

Ensuring that (preferably aggregated) logging is set up across networks and hosts will save some time during active threat events. There are several community-driven signature repositories and low-cost rulesets that can give defenders at least basic visibility into potential intrusions in their environments, along with a plethora of commercial solutions. Knowing ahead of time what kind of visibility you have into suspicious events will drive faster and more effective responses during critical situations.

Harden critical systems.

Harden **critical products** against low-skill and opportunistic attacks. Your virtualization and network infrastructure solutions should be isolated not only from the internet, but from as many internal systems as possible. Make it difficult for attackers to get to the applications that are central to the management of your network and operations.

While it may seem basic, hardening includes ensuring you've changed all default and administrative passwords in technology you implement to be complex and non-standard. Software and solutions you rely on in your environment may have undocumented service or administrative users—though we hope none of these have **hard-coded passwords**. Thorough review and segmentation will slow down attackers. Implement multi-factor authentication (MFA) and monitor authentication events for remote logins.

Define both a regular patching cycle and emergency zero-day patching procedures.

The window for effective patching has decreased in the past two years. Fifty-percent of the vulnerabilities in this report were exploited within seven days of disclosure. It is essential that organizations have emergency patching procedures and incident response playbooks in place in addition to a clearly defined, regular patch cycle that prioritizes actively and widely exploited CVEs. Without an understood, standardized mechanism for driving aligned emergency action, you're at much higher risk from these increasingly frequent events.

In addition to regular and emergency patching procedures,

organizations should ensure they keep current with operating system-level updates, such as Microsoft's **Cumulative Updates** for Windows systems. Failing to ensure timely installation of Cumulative Updates may mean that you are unable to quickly install out-of-band security patches when sudden attacks occur.

The same principle applies to all operating system-level patches, no matter the platform; OS-level vulnerabilities are a boon to attackers, even if they are not exposed to the internet.

Network edge devices (network pivots) continue to be popular and frequently exposed attack surface area. The same goes for network infrastructure targets that offer attackers the ability to compromise downstream devices or resources (e.g., virtualization infrastructure) and email servers like Microsoft Exchange. These categories of software and firmware should adhere to a zero-day patch cycle wherever possible, meaning that updates and/or downtime should be scheduled as soon as new critical or high-severity advisories are released.

As of late 2021, the U.S. Cybersecurity and Infrastructure Agency (CISA) has a list of known-exploited vulns (**KEV**), which they are updating on a regular basis. While the patching deadlines in the KEV list are aimed at government agencies and federal contractors, it's a good idea for non-government organizations to track that guidance and those SLAs closely.

Leverage resources on ransomware prevention and readiness.

The rise of ransomware has changed the security landscape, and organizations should be prepared to implement multilayered defenses against ransomware threats. The Institute for Security and Technology has a comprehensive **framework** for ransomware prevention and readiness developed in partnership with industry experts, **including Rapid7**. CISA also has **in-depth guidance** on readiness and response. Rapid7 has additional ransomware resources **here** and regularly **writes about** ransomware detection and prevention tactics.

Development pipelines are targets—and developers can be, too.

Rapid7's security teams published an in-depth list of **practices for protecting development pipelines** from supply chain attacks. This list covers topics from version control and job-specific credentials for CI jobs to secrets and hash management. It also includes detection and response techniques.

Defense in depth is a more effective strategy than patching alone.

Skilled attackers are resourceful and, at times, utterly opportunistic. They can and will use any tool—any technique, any weakness, any piece of information—to build successful attack chains. Patches are not always effective, either, as evidenced by **CVE-2021-41773**, **CVE-2021-1732**, and Log4Shell CVE-2021-44228, all of which had at least part of their original fixes bypassed.

Additionally, many of the CVEs treated individually in this report can be used in concert with one or more additional vulnerabilities to achieve something beyond the scope of a single CVE's impact. Defenders can get ahead of future attacks by taking care not to treat individual vulnerabilities as if they existed in a vacuum, but instead choosing to implement controls and detection mechanisms across the whole of their environment.

At Rapid7, we believe that research-driven context on vulnerabilities and emergent threats is critical to building forward-looking security programs and advancing community knowledge. Security and IT teams face mounting challenges in a heightened threat climate, and we are committed to partnering with those teams to foster more in-depth understanding of defense-in-depth strategies that will strengthen organizations' security posture, both now and in the future.

For more information on the vulnerabilities featured in this report, and for Rapid7 and community analysis of new vulnerabilities and threats, keep an eye on **AttackerKB**.

Appendix

This dataset does not include all CVEs or even all active threats we evaluated in 2021, but it does represent a diverse sample of attacker use cases and exploitation case studies. Our intent is not to imply that any one CVE or vulnerability group is less important than others. Security teams, network administrators, and defenders at large have in-depth understanding of which assets are critical in their environments and how action taken may affect their business priorities. What we offer is an attacker-centric view of the vulnerability landscape that Rapid7 customers and the security community can use to inform the policies and practices that they employ as part of a larger defense-in-depth strategy.

Full Dataset

CVE	Threat Status	Attacker Utiliity	Vulnerability Class	Time to Known Exploitation (TTKE) in Days
CVE-2021-28799 QNAP HBS 3 Improper Authorization	• Widespread Threat (0day)*	Network pivot	Improper Access Control	0
CVE-2021-27101 Accellion FTA Unauthenticated SQL Injection	• Widespread Threat (0day)	Remote code execution	Injection / SQL	0
CVE-2021-27103 Accellion FTA Server-Side Request Forgery	• Widespread Threat (0day)	Remote code execution	Injection / Request	0
CVE-2021-34527 Microsoft Windows Print Spooler Remote Code Execution "PrintNightmare"	• Widespread Threat (0day)	Remote code execution	Improper Access Control	0
CVE-2021-40444 Microsoft MSHTML Remote Code Execution	• Widespread Threat (0day)	Remote code execution	Injection / ActiveX	0
CVE-2021-26857 Microsoft Exchange Server Unified Messaging Deserialization "ProxyLogon"	• Widespread Threat (0day)	Remote code execution	Deserialization	0
CVE-2021-26858 Microsoft Exchange Server Arbitrary File Write "ProxyLogon"	• Widespread Threat (0day)	Remote code execution	Injection / File	0
CVE-2021-44228 Apache Log4j Unauthenticated Remote Code Execution "Log4Shell"	• Widespread Threat (0day)	Remote code execution	Injection / JNDI	0
CVE-2021-27065 Microsoft Exchange Server Arbitrary File Write "ProxyLogon"	• Widespread Threat (0day)	Remote code execution	Injection / File	0

CVE	Threat Status	Attacker Utility	Vulnerability Class	Time to Known Exploitation (TTKE) in Days
CVE-2021-26855 Microsoft Exchange Server-Side Request Forgery "ProxyLogon"	• Widespread Threat (0day)	Remote code execution	Injection / Request	0
CVE-2021-30116 Kaseya VSA Credential Disclosure	• Widespread Threat (0day)	Information disclosure	Improper Access Control	0
CVE-2021-20021 SonicWall Email Security Pre-Authentication Administrative Account Creation	• Widespread Threat (0day)	Network pivot	Improper Access Control	0
CVE-2021-20016 SonicWall SMA 100 Series Unauthenticated SQL Injection	• Widespread Threat (0day)	Network pivot	Injection / SQL	0
CVE-2021-22893 Pulse Connect Secure Remote Unauthenticated Arbitrary Code Execution	• Widespread Threat (0day)	Network pivot	Memory Corruption	0
CVE-2021-35211 SolarWinds Serv-U Remote Memory Escape	• Widespread Threat (0day)	Remote code execution	Memory Corruption	0
CVE-2021-41773 Apache HTTP Server Path Traversal and Remote Code Execution	• Widespread Threat (0day)	Remote code execution	Improper Access Control	0
CVE-2021-44515 Zoho ManageEngine Desktop Central Authentication Bypass	• Widespread Threat (0day)	Network infrastructure compromise	Improper Access Control	0
CVE-2021-34523 Microsoft Exchange Server Elevation of Privilege "ProxyShell"	• Widespread Threat	Local code execution	Improper Access Control	30
CVE-2021-34473 Microsoft Exchange Server Remote Code Execution "ProxyShell"	• Widespread Threat	Remote code execution	Improper Access Control	30
CVE-2021-31207 Microsoft Exchange Server Security Feature Bypass "ProxyShell"	• Widespread Threat	Remote code execution	Injection / Request	93
CVE-2021-21972 VMware vCenter Server Remote Code Execution	• Widespread Threat	Network infrastructure compromise	Improper Access Control	7

CVE	Threat Status	Attacker Utility	Vulnerability Class	Time to Known Exploitation (TTKE) in Days
CVE-2021-22205 GitLab Unauthenticated Remote Code Execution	• Widespread Threat	Remote code execution	Improper Access Control	48
CVE-2021-26084 Atlassian Confluence Server Webwork OGNL Injection	• Widespread Threat	Remote code execution	Injection / OGNL	7
CVE-2021-35464 ForgeRock AM Unauthenticated Remote Code Execution	• Widespread Threat	Remote code execution	Deserialization	7
CVE-2021-42237 Sitecore Unauthenticated Remote Code Execution	• Widespread Threat	Remote code execution	Deserialization	28
CVE-2021-36942 Microsoft Windows LSA Spoofing "PetitPotam Attack"	• Widespread Threat	Network infrastructure compromise	Improper Access Control	33
CVE-2020-6207 SAP Solution Manager Missing Authentication Check	• Widespread Threat	Network infrastructure compromise	Improper Access Control	Unknown
CVE-2021-44077 Zoho ManageEngine ServiceDesk Plus Unauthenticated Remote Code Execution	• Widespread Threat	Remote code execution	Improper Access Control	67
CVE-2021-22986 F5 iControl REST Unauthenticated Remote Command Execution	• Widespread Threat	Network pivot	Injection / Command	9
CVE-2021-22005 VMware vCenter Server Arbitrary File Upload	• Widespread Threat	Network infrastructure compromise	Injection / Request	3
CVE-2021-21985 VMware vCenter Server Remote Code Execution	• Widespread Threat	Network infrastructure compromise	Injection / JNDI	10
CVE-2020-29583 Zyxel USG Hardcoded Admin Credential	• Widespread Threat	Network pivot	Improper Access Control	14
CVE-2021-38647 Microsoft Azure Open Management Infrastructure Remote Code Execution "OMIgod"	• Widespread Threat	Remote code execution	Improper Access Control	2

CVE	Threat Status	Attacker Utiliity	Vulnerability Class	Time to Known Exploitation (TTKE) in Days
CVE-2021-30657 Apple macOS Gatekeeper Bypass	• Exploited in the wild (0day)	Local code execution	Improper Access Control	0
CVE-2021-40539 Zoho ManageEngine ADSelfService Plus Authentication Bypass	• Exploited in the wild (0day)	Remote code execution	Improper Access Control	0
CVE-2021-1732 Microsoft Windows Win32k Elevation of Privilege	• Exploited in the wild (0day)	Local code execution	Memory Corruption	0
CVE-2020-7961 Liferay Portal Unauthenticated Remote Code Execution	• Exploited in the wild	Remote code execution	Deserialization	Unknown
CVE-2021-21975 VMware vRealize Operations Manager API Server-Side Request Forgery	• Exploited in the wild	Network infrastructure compromise	Improper Access Control	Unknown
CVE-2021-21551 Dell dbutil Driver Insufficient Access Control	• Exploited in the wild	Local code execution	Improper Access Control	13
CVE-2021-21307 Lucee Administrator Unauthenticated Remote Code Execution	• Exploited in the wild	Remote code execution	Improper Access Control	Unknown
CVE-2021-36934 Microsoft Windows Elevation of Privilege "Serious SAM"	• Exploited in the wild	Local code execution	Improper Access Control	Unknown
CVE-2021-1497 Cisco Hyperflex HX Command Injection	• Exploited in the wild	Network infrastructure compromise	Injection / Command	31
CVE-2021-40438 Apache HTTP Server Server-Side Request Forgery	• Exploited in the wild	Network infrastructure compromise	Injection / SSRF	69
CVE-2021-2394 Oracle WebLogic Server Remote Code Execution	• Impending - High-value target	Remote code execution	Deserialization	N/A

CVE	Threat Status	Attacker Utiliity	Vulnerability Class	Time to Known Exploitation (TTKE) in Days
CVE-2021-43287 GoCD Pre-Authenticated Build Pipeline Takeover	• **Impending** - High-value target	Information disclosure	Improper Access Control	N/A
No CVE Microsoft Azure Cosmos DB Unauthorized Privileged Access "ChaosDB"	• **Impending** - High-value target	Network infrastructure compromise	Improper Access Control	N/A
CVE-2020-7388 Sage X3 ERP Remote Code Execution	• **Impending** - Exploit available	Remote code execution	Improper Access Control	N/A
CVE-2021-26914 NetMotion Mobility Arbitrary Code Execution	• **Impending** - Exploit available	Network pivot	Deserialization	N/A
CVE-2021-34481 Microsoft Windows Print Spooler Remote Code Execution	• **Impending** - Exploit available	Remote code execution	Injection	N/A
CVE-2020-25223 Sophos UTM Remote Code Execution	• **Impending** - Exploit available	Network pivot	Injection / Command	N/A

Notes on Methodology

With very few exceptions, CVEs featured in this report were either disclosed or exploited in the wild in 2021. The CVEs we have categorized as exploited in the wild in this report are not the only vulnerabilities actively exploited during the 2021 calendar year. For example, we have excluded many browser and host-based vulnerabilities known to be exploited in the wild (e.g., bugs in Internet Explorer, Chrome, and Firefox). Google Project Zero has a spreadsheet of some other zero-days exploited in the wild in 2021 here.

CVSS scores have been removed from our 2021 dataset. CVSS score can be a useful metric, but we believe other forms of metadata, such as threat status and attacker utility, are more important for risk assessment and prioritization than CVSS alone.

Since the trustworthiness of our data is important, we cite primary sources wherever possible for vulnerabilities we've listed as exploited in the wild—that is, we reference firsthand accounts of exploitation from the organizations or individuals who detected, verified, and reported them. Examples of primary sources referenced throughout this paper include U.S. cybersecurity and intelligence agency alerts on known exploitation; security firm analyses of threats and IOCs they've tracked during incident response or other investigations; and vendor advisories that specify exploitation in the wild (this includes CVEs that are disclosed as zero-days).

In the interest of readability, in some cases we also cite articles in security news publications that aggregate disparate reports of exploitation. This is especially useful when certain vulnerabilities, like the ProxyLogon or PrintNightmare CVEs, are so widely exploited that it is difficult to track firsthand accounts. Our goal in citing news sources is to allow readers to understand the volume and impact of exploitation as quickly as possible.

Threat Categorization

Widespread threats are vulnerabilities under attack by many bad actors. Ransomware is by nature an at-scale operation; it relies on volume to succeed, whether that volume occurs in the ransoms individual groups levy or the number of organizations under attack. Because it is both tempting and likely that the former will turn into the latter, we are now categorizing *any* CVE that has been leveraged by ransomware operators as a widespread threat even if the documented number of ransomware threat actors using that CVE is (initially) small.

Threats categorized as "exploited in the wild" are, quite simply, not known to be broadly exploited at time of writing. It is possible that evidence exists but has not been shared.

Likewise, while we do not have evidence at time of writing that CVEs in our **impending threat** category are exploited in the wild, lack of evidence does not mean absence of exploitation (e.g., **CVE-2021-2394**, **CVE-2020-25223**).

Ransomware Citations

We use security news articles frequently to document ransomware operators' use of specific CVEs. Ransomware citations in this report are a binary—either there is credible technical evidence of ransomware groups' usage of a vulnerability or there is not. Lack of confirmation does not mean a CVE has not been used in ransomware operations, only that we have not seen reproducible details supporting that conclusion. Credible sources typically include some combination of original analysis (e.g., **CVE-2021-20021**, **CVE-2021-27103**), news articles that aggregate primary sources (**CVE-2021-26084**, **CVE-2021-34527**), and expert commentary on open platforms (**ProxyLogon**, more **ProxyLogon**). In general, when a report comes from an individual or a little-known entity rather than a recognized expert, we look for technical information like payloads, source IPs, and attack chain analysis to support the claim.

Calculating Time to Known Exploitation (TTKE)

Compiling and communicating timelines is one of the most difficult parts of risk assessment. When calculating Time to Known Exploitation (TTKE), wherever possible we use the first credible public reference to a vulnerability's existence and the first credible public reference to exploitation in the wild. Often the first and most authoritative source on the existence of new CVEs is a vendor advisory, but in this age of widespread zero-day exploitation and public discourse, community references can pre-date vendor bulletins. **CVE-2021-36942**, **CVE-2021-36934**, and Microsoft's "ChaosDB" **vulnerability** are examples of this. Rarely if ever do we use sources like the National Vulnerability Database (NVD) for disclosure baseline dates, since those dates tend to be several days or even weeks behind public (and therefore attacker) knowledge.

Important note: The first known report of exploitation is just that—the first known report. It's possible, and in some cases likely, that exploitation began before a public analysis was released (e.g., **CVE-2021-22205**, **CVE-2021-36942**). TTKE data should not be taken as evidence that a vulnerability was NOT exploited before the observed date.

Glossary of Terms

Attacker Utilities

Remote code execution (RCE): Code execution on a remote target. Typically refers to the ability to execute a payload on a target system (e.g., obtain a shell session). Aids in credential stealing, data exfiltration, and so on.

Local code execution: The ability to run code locally on a system to which the attacker already has some access. Most commonly used to escalate privileges (e.g., by executing code as the user running the vulnerable application).

Network infrastructure compromise: Compromise of networked infrastructure, such as a network management system or backup system, that may give an attacker access to everything managed by that software. Vulnerabilities in virtualization, automation, and/or device management infrastructure all fall into this category.

Network pivot: The ability to pivot from an external network to an internal network, most often by exploiting internet-facing systems such as VPNs, firewalls, routers, and other gateway devices. A network pivot gives an attacker visibility into both internal and external traffic and aids in data exfiltration, traffic sniffing, and further attacks within the target network.

File enumeration: The ability to enumerate files on a target. File reads do not give an attacker a path to code execution by themselves, but instead function as primitives that allow attackers to gather information that enables a secondary part of an exploit chain (e.g., remote code execution). Can aid in turning a post-authentication vulnerability into a pre-authentication vulnerability.

Vulnerability Classes

Deserialization is the process through which an application is able to convert data from a portable format to data types native to its own language. Many modern languages support deserialization, including Java, .NET, Python, and Ruby. The deserialization process can pose a threat to security when the data that is loaded into the native language can be tampered with by a malicious party. Typical attacks involve configuring the data to invoke a method with the arguments necessary to execute an operating system command. This results in command execution in the context of the loading application. Common solutions to this security problem include cryptographically signing the data to ensure its authenticity and utilizing an allowlist of data types that are permitted to be loaded. Associated CWEs: CWE-502.

Improper Access Control refers to a missing or insufficient access control to a particular interface into a system (most often a remotely accessible API). Improper uses of cryptography for the purpose of authentication also fall under this vulnerability class. Common solutions to this problem include proper authentication, authorization, and accounting implementations for all sensitive interfaces, as well as secure management of all related secrets. A non-exhaustive list of associated CWEs: CWE-285, CWE-200, CWE-287, CWE-732.

Memory Corruption is a large category of vulnerabilities that involve the misuse of data through a variety of means to alter memory and produce unexpected behavior. This vulnerability class includes improper boundary enforcement, type confusion, uninitialized data use, and the use of data after it has been freed, to name a few. These vulnerabilities often manifest themselves in languages that are not considered “type-safe.” Successful exploitation of memory corruption vulnerabilities can result in arbitrary code execution within the context of the running application, or in an unhandled exception that causes the application to crash and triggers a denial of service (DoS) condition. Common solutions to this problem typically involve additional validation on parameters to key operations, such as those used to load and store data. Successful exploitation of these classes of vulnerabilities has become more complex in recent years due to the variety of countermeasures and safeguards that have been developed, such as kASLR, Control Flow Guard, win32k Type Isolation, and so on. A non-exhaustive list of associated CWEs: CWE-787, CWE-125, CWE-416, CWE-190, CWE-476.

Injection is a large category of vulnerabilities involving specially crafted input that is interpreted in a particular way by an associated system. Most commonly seen in web applications, injection attacks are often more specifically labeled by the type of data being interpreted (e.g., SQL, LDAP, OS commands). The root cause of these vulnerabilities is almost always insufficient sanitization on data received from a malicious party. Exploitation of these vulnerabilities tends to be reliable, rarely resulting in service degradation unless intended (such as through SQL or OS commands). Our 2021 report includes JNDI, OGNL, SSRF, and other techniques we have classified as injection flaws in addition to traditional OS and SQL command injection vulnerabilities.

The context under which the logic is executed typically depends on how it is interpreted. In the case of a web application, for example, SQL injection may be executed on a back-end database server, while OS commands are injected on the front-end web server, and JavaScript is executed by the end user's browser. This class of vulnerabilities is therefore unique in that it commonly involves a vulnerability in one system compromising the integrity of others. Common solutions to this problem typically involve implementing strict sanitization on parameters though the use of allowlists. A non-exhaustive list of associated CWEs: CWE-79, CWE-20, CWE-89, CWE-94.

References

Security research is a community pursuit. This report benefited from the work of many individual researchers and research teams, including but not limited to the work of the folks listed below:

0x80O0oOverfl0w (2021)
Aaron Soto and Jon Hart, Rapid7 (2019)
Andrew Christian, Rapid7 (2021)
Andrew Moore, Genevieve Stark, Isif Ibrahima, Van Ta, Kimberly Goody, Mandiant (2021)
Andy Rector (2020)
Apple Support (2021)
Arianne Dela Cruz, Cris Tomboc, Jayson Chong, Nikki Madayag, Sean Torre, Trend Micro (2021)
ATT&CK, Mitre (2020)
ATT&CK, Mitre (2021)
Australian Cybersecurity Centre (2021)
Australian Cybersecurity Centre (2021)
Bad Packets (2021)
Bad Packets (2021)
Ben Hawkes, Project Zero (2019)
Benjamin Delpy (2021)
Bill Whitaker, CBS News (2021)
Bob Rudis Rapid7 (2021)
Bob Rudis Rapid7 (2021)
Bob Rudis, Rapid7 (2021)
Bob Rudis, Rapid7 (2021)
Brendan Watters, Rapid7 (2021)
Caitlin Condon, Spencer McIntyre, Will Vu, Rapid7 (2020)
Cedric Owens (2021)
Charlie Osbourne ZDNet (2021)
Chris Caridi and Allison Wikoff, Security Intelligence (2021)
Christophe De La Fuente, Rapid7 (2021)
Christopher Bing, Reuters (2021)
Cisco (2021)
Cisco Security Advisories (2021)
Codecov (2021)
Cyber Security & Infrastructure Security Agency (2021)
Cyber.dhs.gov (2021)
Cybersecurity & Infrastructure Security Agency (2021)
Cybersecurity & Infrastructure Security Agency (2021)
Cybersecurity & Infrastructure Security Agency (2021)
Cybersecurity & Infrastructure Security Agency (2021)
Cybersecurity & Infrastructure Security Agency (2021)
Cybersecurity & Infrastructure Security Agency (2021)
Cybersecurity & Infrastructure Security Agency (2021)
Cybersecurity & Infrastructure Security Agency (2021)
Cybersecurity & Infrastructure Security Agency (2021)
Cybersecurity & Infrastructure Security Agency (2021)
Cybersecurity & Infrastructure Security Agency (2022)
Damian Menscher (2021)
Dan Goodin, Ars Technica (2021)
Dan Goodin, Ars Technica (2021)
Dan Perez, Sarah Jones, Greg Wood, Stephen Eckels, Mandiant (2021)
Danny Palmer, ZDNet (2021)
Danny Palmer, ZDNet (2021)
Dark Reading Staff, Dark Reading (2021)
Deadjakk (2021)
Dennis Fisher, Duo Security (2021)
Desktop Central, Manage Engine (2021)
Dhwani Meharchandani, Security Boulevard (2021)
Dutch Institute for Vulnerability Disclosure CSIRT (2021)
Dylan Codes (2021)
Erick Galinkin, Rapid7 (2021)
F5 (2021)
F5 Labs (2021)
F5 Labs (2021)
FBI Flash (2021)
FBI Flash (2021)
FBI Flash (2021)
Fortiguard Labs, Fortinet (2021)
Frank Breedijk, DIVD CSIRT (2021)
Gentilkiwi (2020)
GitHub Advisory Database (2021)
Glenn Thorpe, Rapid7 (2021)
Glenn Thorpe, Rapid7 (2021)
GoCD (2021)
Grant Wilcox, Rapid7 (2021)
Grant Wilcox, Rapid7 (2021)
GreyNoise (2021)
Healey Library, University of Massachusetts Boston (2022)
HHS Cybersecurity Program (2021)
Ionut Ilascu, Bleeping Computer (2021)
IoT Inspector (2021)
Jack Heysel, Rapid7 (2021)

Jake Baines, Rapid7 (2021)
Jake Baines, Rapid7 (2022)
Jake Baines, Rapid7 (2021)
Jake Baines, Rapid7 (2021)
Jake Baines, Rapid7 (2021)
Jesse Mack, Rapid7 (2021)
Johannes Ullrich, Internet Storm Center (2021)
John Hammond, Huntress (2021)
Jonas L (2021)
Jordan Nuce, Jeremy Kennelly, Kimberly Goody Andrew Moore, Alyssa Rahman, Matt Williams, Brendan Mckeague, Jared Wilson, Mandiant (2021)
Josh Fleischer, Chris DiGiamo, AlexPennino, Mandiant (2021)
Josh Grunzweig, Matthew Meltzer, Sean Koessel, Steven Adair, Thomas Lancaster, Volexity (2021)
Justin Pagano, Rapid7 (2021)
Kaseya (2021)
Kevin Beaumont (2021)
Kevin Beaumont (2021)
Kevin Beaumont (2021)
Kevin Beaumont (2021)
Kevin Beaumont (2021)
Kevin Beaumont (2021)
Kevin Beaumont, Double Pulsar (2021)
Kevin Beaumont, Double Pulsar (2021)
Kiteworks (2021)
Kurt Mackie, Redmond (2021)
Lawrence Adams, Bleeping Computer (2021)
Lily Hay Newman, Wired (2021)
Lisa Vaas Threatpost (2022)
Mia Jankowicz and Charles R. Davis, Business Insider (2021)
Michael Gillespie (2021)
Michael Gillespie (2021)
Microsoft (2009)
Microsoft (2021)
Microsoft (2021)
Microsoft (2021)
Microsoft (2021)
Microsoft (2021)
Microsoft (2021)
Microsoft (2022)
Microsoft 365 Defender Threat Intelligence Team, Microsoft Threat Intelligence Center (2021)
Microsoft 365 Defender Threat Intelligence Team, Microsoft Threat Intelligence Center, Microsoft 365 Security (2021)
Microsoft Security Response Center (2021)
Microsoft Security Response Center (2021)
Microsoft Security Response Center (2021)
Microsoft Security Response Center (2021)
Microsoft Security Response Center (2021)
Microsoft Security Response Center (2021)
Microsoft Security Response Center (2021)
Microsoft Security Response Center (2021)
Microsoft Threat Intelligence Center (2021)
Microsoft Threat Intelligence Center (MSTIC), Microsoft 365 Defender Threat Intelligence Team, Microsoft 365 Security (2021)
Microsoft Threat Intelligence Center (MSTIC), Microsoft 365 Defender Threat Intelligence Team, Microsoft 365 Security (2021)
Microsoft Threat Intelligence Center, Microsoft 365 Defender Threat Intelligence Team, Microsoft365 Security (2021)
Mike Hanley, GitHub (2021)
Millers-crossing (2021)
MITRE (2021)
MITRE (2021)
Mounir Hahad and Alex Burt, Juniper Networks (2021)
National Cybersecurity Authority (2021)
National Telecommunications and Information Administration (2021)
National Vulnerability Database (2021)
National Vulnerability Database (2021)
Neville O'Neill, Rapid7 (2021)
Nikita Popov, The PHP Group (2021)
NinjaOperator (2021)
Nir Ohfeld and Sagi Tzadik, Wiz (2021)
Omer Ventura, Ori Hamama, Network Research, Checkpoint Research (2021)
Oracle (2021)
Orange Tsai, Devcore Security Consulting (2021)
OWASP (2021)
OWASP (2021)
Patrick Howell O'Neill, MIT Technology Review (2021)
Patrick Wardle, Objective-See (2021)
Paul Kimayong, Juniper Networks (2021)
Peleg Hadar and Tomer Bar, SafeBreach Labs (2020)
PetitPotam (2021)
Philip Misner (2021)

Piergiovanni Cipolloni, HN Security (2021)
Podalirius (2021)
Project Zero (2021)
Proxylogon (2021)
Ransomware Task Force, Institute for Security & Technology (2021)
Rapid7 (2021)
Rapid7 (2021)
Rapid7 (2021)
Rapid7 (2021)
Rapid7 (2021)
RedCursorSecurityConsulting (2021)
Research and Intelligence Fusion Team, NCC Group (2021)
Research and Intelligence Fusion Team, NCC Group (2021)
Research Intelligence and Fusion Team, NCC Group (2021)
Rootsecdev (2021)
Rootxharsh (2021)
Rui, Deniable (2020)
Satoshi Tanda, Crowdstrike (2021)
Satoshi Tanda, Crowdstrike (2021)
Sergiu Gatlan, Bleeping Computer (2021)
Sergiu Gatlan, Bleeping Computer (2021)
Sergiu Gatlan, Bleeping Computer (2021)
Sergiu Gatlan, Bleeping Computer (2021)
Sergiu Gatlan, Bleeping Computer (2021)
Shadowhunter Lab, DBapp Security (2021)
Shelby Pace, Rapid7 (2021)
Siddharth G, Pit Stop ManageEngine (2021)
Solarwinds (2021)
Sonicwall (2021)
Spencer McIntyre, Rapid7 (2021)
Stan Hegt (2021)
SwiftOnSecurity (2021)
The DFIR Report (2021)
Threat Hunter Team, Symantec (2021)
Threat Hunter Team, Symantec (2021)
Tod Beardsley, Rapid7 (2021)
Tom Burt, Microsoft (2021)
Topotam (2021)
Topotam (2022)
VMWare (2021)
Wikipedia (2017)
Will Dormann (2021)
Will Dormann (2021)
Will Dormann (2021)
Will Schroeder, SpecterOps (2021)
Will Vu, Rapid7 (2021)
Will Vu, Rapid7 (2021)
Will Vu, Rapid7 (2021)
Will Vu, Rapid7 (2021)
Will Vu, Rapid7 (2021)
Will Vu, Rapid7 (2021)
Will Vu, Rapid7 (2021)
Will Vu, Rapid7 (2021)
Will Vu, Rapid7 (2021)
Will Vu, Rapid7 (2021)
Will Vu, Rapid7 (2021)
Will Vu, Rapid7 (2021)
Will Vu, Rapid7 (2021)
Will Vu, Rapid7 (2021)
Will Vu, Rapid7 (2021)
Will Vu, Rapid7 (2021)
William Vu Rapid7 (2021)
William Vu, Rapid7 (2021)
Wiz (2021)
Yolkan Yazici (2021)
Zeljka Zorz, Help Net Security (2020)
Zeljka Zorz, Help Net Security (2021)
Zero Day Initiative (2021)

HEFESTIS Weekly Newsletter

A very warm welcome to all of you from all of us at the CISO-Share Office.

For those that attended the UCISA Bett conference this year we hope you were able to attend the panel discussing "Cybersecurity and Risk Assessment: Protecting your institution in the information age" that David was on. As the supporting material is released we will let you know where to find it.

The latest on the HW incident is that containment is in place with no reports of lateral spread. The investigation into the incident is ongoing and that the offers of support are greatly appreciated. Further updates will be included on CiSP and directly from official communications channels, we will also continue to inform as directed by the incident and communications teams.

Please check the CiSP site, as always, for the latest updates on current incidents and countermeasures to protect your institution.

Whilst you are there, why not drop into the CISO-Share user forum and discuss the latest topics and news.

Here are a few of the articles which caught the attention of the CISO-Share team this week.

If you have any questions or comments please feel free to contact us via CISO-Office@hefestis.ac.uk.

Here are some of the week's Cyber Security articles which caught the attention of CISO-Share.

Cyberattack Tools Sell for Under $50 on the Dark Web

https://www.digit.fyi/cyberattack-tools-sell-for-under-50-on-dark-web/

Tools and equipment that allow hackers to perform any type of cyberattack are being sold for as little as $50 on the dark web. The kits enable people with little technical knowledge to launch cyberattacks.

Cyberattack packs, including phishing, ransomware, DDoS, and others, were available for sale on the dark web. While most cost less than $50, were found some starting as low as $5.

Prices of basic ransomware, which employs encryption to hold victims' data at ransom, start at $15.

Action Point:

The cost of launching attacks is decreasing with little skill needed to buy and run these tools. The linked article has the current costs of attack tools found on the dark web for many more attacks, including malware and VPN attacks. Visit the site to learn more about the minimal costs involved in launching attacks.

Have they bust the LAPSUS$ gang?

https://nakedsecurity.sophos.com/2022/03/25/uk-police-arrest-7-hacking-suspects-have-they-bust-the-lapsus-gang/

Seven suspected hackers (between the ages of 16 and 21) have been arrested in the UK, with many headlines insisting that this is a "LAPSUS$ bust". At present there is nothing that explicitly connects these arrests with the DEV-0537 a.k.a. LAPSUS$ group. *Lapsus*, which is as good a Latin word as any for "data breach", followed by a *dollar sign.*

This group has been attributed a flurry of recent attacks that have made the headlines. Including successful attacks against Microsoft and Okta.

Early observed attacks by DEV-0537 targeted cryptocurrency accounts resulting in compromise and theft of wallets and funds. They have also been observed targeting government entities, manufacturing, higher education, energy, retailers, and healthcare.

Action Point:

Heightened monitoring and awareness of the current increased cyber-attack activity is essential. Continue to progress information and cyber security programs prioritising work in light of lessons learned from recent attacks.

Brits Express Greater Concern Over Data Privacy as Cyber Attacks Soar

https://www.itgovernance.co.uk/blog/brits-express-greater-concern-over-data-privacy-as-cyber-attacks-soar

Three quarters of UK residents are concerned about their online safety, according to a study by the cyber security firm Surfshark.

That figure might not come as a surprise, given the growing awareness of data privacy. There are regular news stories of data breaches, while the GDPR (General Data Protection Regulation) has changed the way organisations handle personal data.

Yet, what is a surprise is what we are doing to address these concerns. Surfshark found that, compared to respondents in Australia, Canada, Germany and the US, Brits are the least likely to use data privacy tools such as antivirus software and ad blockers.

Action Point:

IT Governance continue that if organisations and individuals are to better protect themselves online and mitigate the risk of their personal information being misused, we must all gain a better

understanding of the threat landscape and the steps we can take to protect ourselves. We could not agree more.

New Phishing Technique to Spoof a Legitimate Domain

https://cybersecuritynews.com/bitb-attack/

Recently, a new phishing technique, BitB attack has been discovered that is so well designed that most people would fall for it.

By spoofing a legitimate domain using this attack, it is possible to stage convincing phishing attacks that mimic a website window within the browser.

With the BitB attack, an entirely fabricated browser window is created by combining HTML and CSS. Social engineering campaigns can be easily mounted using this method. While the phishing domain holding a fake authentication window is necessary for credential harvesting since potential victims need to be redirected to it.

Action Point:

Cybersecurity researchers have recommended a few mitigations:

- Always use one of the best password managers.
- Always use robust antivirus.
- Make sure to enable multifactor authentication.
- Always monitor the system and network logs.
- Try to resize or scroll the pop-up window to verify the authenticity of the Window.
- Make sure to implement best security practices.

---

6 steps to getting risk acceptance right

https://www.csoonline.com/article/3653312/6-steps-to-getting-risk-acceptance-right.html

Know what's most important to your organisation
Understand which risks pose what concerns allows for informed conversations about the risks the organisation is willing to accept.

Analyse, communicate risks with a business lens
Put cyber risks into business context. That way C-suite colleagues can delineate which risks they want to avoid, transfer, mitigate, and accept.

Engage the business on risk acceptance
The executives who own the business areas impacted by the risk should be the ones to determine which risks the organisation wants to avoid, transfer, mitigate or accept. Then it needs to be debated all the way up through the risk committee and then the board, who can sign off on it.

Let the business own the risk, but remain partners in managing it
Because setting risk acceptance is a business exercise, management and ownership of it should rest with the roles or teams responsible for the functions, services, or products impacted by the risk.

Employ frameworks, tools to support risk management
Use a risk management methodology, to direct, manage, and track these activities.

Revisit and re-evaluate risk acceptance
Organisations need to evaluate their appetite for risk, and with it their risk acceptance levels, on a regular basis; annually or more often, as changing circumstances might require.

Action Point:
Try and continually stay in touch with business to understand how risk should be accepted or not. Ideally, we want to strive to get to a place where we're continually understanding that and how we need to change our approach.

Act Now to Protect Against Potential Cyberattacks

https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/21/fact-sheet-act-now-to-protect-against-potential-cyberattacks/

The White House has urged companies in the U.S. to execute the following steps with urgency:

- Mandate the use of multi-factor authentication on your systems to make it harder for attackers to get onto your system;
- Deploy modern security tools on your computers and devices to continuously look for and mitigate threats;
- Check with your cybersecurity professionals to make sure that your systems are patched and protected against all known vulnerabilities, and change passwords across your networks so that previously stolen credentials are useless to malicious actors;
- Back up your data and ensure you have offline backups beyond the reach of malicious actors;
- Run exercises and drill your emergency plans so that you are prepared to respond quickly to minimize the impact of any attack;
- Encrypt your data so it cannot be used if it is stolen;
- Educate your employees to common tactics that attackers will use over email or through websites, and encourage them to report if their computers or phones have shown unusual behaviour, such as unusual crashes or operating very slowly; and
- Engage proactively with your local FBI field office or CISA Regional Office to establish relationships in advance of any cyber incidents. Please encourage your IT and Security leadership to visit the websites of CISA and the FBI where they will find technical information and other useful resources.

Action Point:
Very similar points the advice already distributed by the NCSC, ENISA and ourselves. For the last point ensure that your recovery plans have the contact details for our Scottish and UK based organisation that will need to be informed and can help in response activities.

FBI warns of cyberattacks using AvosLocker ransomware

https://www.techrepublic.com/article/fbi-warns-cyberattacks-avoslocker-ransomware/

The AvosLocker Ransomware as a Service (RaaS) group has targeted critical infrastructure sectors in the US, such as financial services, manufacturing and government facilities, the FBI said.

The FBI and US Treasury are advising organizations to beware of a specific strain of ransomware aimed at critical infrastructure sectors in the United States. Published last Thursday, a joint cybersecurity advisory issued by the two agencies warns of a Ransomware as a Service (RaaS) affiliate-based group known as AvosLocker.

Victims include but aren't limited to financial services, manufacturing and government agencies. The group claims it has targeted organizations not just in the US but in the UK, Canada, China, Taiwan, Germany, Spain, Saudi Arabia and other nations.

This particular ransomware encrypts files on a victim's server, renaming them with an extension of .avos, avos2 or AvosLinux. Named GET_YOUR_FILES_BACK.txt, the ransom note tells victimized organizations that their files and confidential documents have been encrypted and that they must pay for a decryption key and application. Victims are then instructed to browse to an AvosLocker .onion payment site to make the ransom payment in Monero (or Bitcoin at a 10%-25% premium).

Action Point:

RAAS with telephone support and bit-currency options to give you a discount on payment - the audacity of cyber criminals has never been greater.

All the best from all of us at **HEFESTIS** and look out for our next **Threatscape** update next week.

HEFESTIS Weekly Newsletter

A very warm welcome to all of you from all of us at the CISO-Share Office.

Thanks to all our members who have reached out to support the incident reported earlier this week Investigation is ongoing and we are sure that if and as any additional support areas are identified, the sector will do all that it can to assist.

Heriot-Watt University have released a holding page which has been shared via twitter

https://www.hw.ac.uk/uk/services/is/system-status.htm

where further public updates will be provided as they are authorised. Detailed information relating to the incident remains confidential until release via official channels.

We can confirm that containment measures remain in place with no reports of lateral spread or similar malicious activity elsewhere at this time.

The external ports implicated in the attack are

108.61.173.214 /

185.169.233.198 /

104.238.222.158

Please note that Registers of Scotland report that the 104.238.222.158 address is known in VirusTotal as being linked to the ransomware group Lapsus$.

We include information on the Lapsus$ group in this issue with some advice on cyber hygiene and a link to tools in our SharePoint site which may be helpful in assessing risk during and incident.

Further updates will be included on CiSP and directly from official communications channels we will also continue to inform as directed by the incident and communications teams.

Please check the CiSP site, as always, for the latest updates on current incidents and countermeasures to protect your institution.

Whilst you are here, why not drop into the CISO-Share user forum and discuss the latest topics and news.

Additional articles which may be of interest are included with this week's issue.

Ransomware/Incident Risk Assessment And Quantification Tools

Just a quick reminder that we have a number of tools in the Sharepoint library which can support risk analysis in the event of a cyber security incident.

https://hefestis.sharepoint.com/sites/CISOShare/Shared%20Documents/Library/CISO-Share%20Tools

Is Your Browser Clean?

PAM ensures we all know to use separate, secure passwords and privileged accounts when accessing sensitive systems or performing administration on our applications - but are we using a separate or secure browser when we switch?

Browser caches can also store password credentials or use vulnerable password storage applications to hold account details. However convenient it may seem to have your passwords automatically completed; this may make a malicious attackers job easier.

A good, secure password manager can help resolve this issue - and good cyber hygiene can help close the gap.

Useful links

Securing Your Web Browser

What is cyber hygiene and why is it important?

Managing Web Browser Security

Action Point: Privilege account management good practice keeps standard and privileged accounts truly separated and secure.

The Lapsus$ Hacking Group Is Off to a Chaotic Start

Telegram polls. Unusual demands. The latest extortion gang is on an unorthodox rampage.

Main Article

Ransomware gangs have become well-oiled moneymaking machines in their quest for criminal profit. But since December, a seemingly new group called Lapsus$ has added chaotic energy to the field, cavorting about with a strong social media presence on Telegram, a string of high-profile victims—including Samsung, Nvidia, and Ubisoft—calamitous leaks, and dramatic accusations that add up to a reckless escalation in an already unlawful industry.

What makes Lapsus$ noteworthy, too, is that the group isn't really a ransomware gang. Instead of exfiltrating data, encrypting target systems, and then threatening to leak the stolen information unless the victim pays up, Lapsus$ seems to exclusively focus on the data theft and extortion. The group gains access to victims through phishing attacks, then steals the most sensitive data it can find without deploying data-encrypting malware.

Action Points: Easier said than done but -

One of Lapsus$'s trademark antics is to run polls on its Telegram channel where onlookers can vote for whose data the gang should publish next.

Veeam Backup & Replication Multiple Vulnerabilities Reported

CVE-2022-26500 | CVE-2022-26501

Multiple vulnerabilities (CVE-2022-26500, CVE-2022-26501) in Veeam Backup & Replication allow executing malicious code remotely without authentication. This may lead to gaining control over the target system.

Severity: Critical CVSS v3 score: 9.8

Cause

The Veeam Distribution Service *(TCP 9380 by default)* allows unauthenticated users to access internal API functions. A remote attacker may send input to the internal API which may lead to uploading and executing of malicious code.

Solution

Patches are available for the following Veeam Backup & Replication versions:

- *11a (build 11.0.1.1261 P20220302)*
- *10a (build 10.0.1.4854 P20220304)*

Action Points:

- The patch must be installed on the Veeam Backup & Replication server. Managed servers with Veeam Distribution Service will be updated automatically after installing the patch.
- All new deployments of Veeam Backup & Replication version 11a and 10a installed using the ISO images dated 20220302 or later are not vulnerable.
- If you are using Veeam Backup & Replication 9.5, please upgrade to a supported product version.
- Temporary mitigation of the vulnerabilities: Stop and disable the Veeam Distribution Service. The Veeam Distribution Service is installed on the Veeam Backup & Replication server and servers specified as distribution servers in Protection Groups.

Russia State-Sponsored Hackers Used Misconfigured MFA to Breach NGO

FBI and CISA warn of attack on multifactor authentication account to exploit "PrintNightmare" exploit.

Russia State-Sponsored Hackers Used Misconfigured MFA to Breach NGO

Russian State-Sponsored Cyber Actors Gain Network Access by Exploiting Default Multifactor Authentication Protocols and "PrintNightmare" Vulnerability | CISA

Russian nation-state hackers last spring capitalized on a misconfigured Cisco Duo multifactor authentication (MFA) account at a nongovernment organization and created their own device, with MFA, to infiltrate the victim's network, the FBI and Cybersecurity and Infrastructure Security Agency (CISA) warned this week in a joint advisory.

Russian state-sponsored cyber actors gained initial access [TA0001] to the victim organization via compromised credentials [T1078] and enrolling a new device in the organization's Duo MFA. The actors gained the credentials [TA0006] via brute-force password guessing attack [T1110.001], allowing them access to a victim account with a simple, predictable password.

The victim account had been un-enrolled from Duo due to a long period of inactivity but was not disabled in the Active Directory. As Duo's default configuration settings allow for the re-enrolment of a new device for dormant accounts, the actors were able to enrol a new device for this account, complete the authentication requirements, and obtain access to the victim network.

Action Points:

- The FBI and CISA recommend reviewing MFA policies to prevent such a re-enrollment action, confirming that inactive accounts are disabled in Active Directory and MFA systems, and making sure all software is updated, patched, and not prone to known flaws.

Four key risks exacerbated by Russia's invasion of Ukraine

"Russia's invasion of Ukraine has increased the velocity of many risks we have tracked on a quarterly basis in our Emerging Risks survey," said Matt Shinkman, VP with the Gartner Risk and Audit Practice.

There are four major areas of risk that leaders should continually monitor and examine their mitigation strategies as part of a broader aligned assurance approach as the war continues:

Main Article

Talent risk

Employees or students could have family and close friends at risk in the region. Internal communications addressing well-being and outlining counselling services will need to be carefully calibrated and distributed at a higher frequency.

Cybersecurity risk

The potential for increased cybersecurity attacks during this time means that the frequency of tabletop exercises should be increased, as well as ongoing review of protocols to defend against ransomware and other malware attacks.

Financial risk

In the event of direct financial exposure to Russia, there should be close communication with third-party service providers on how best to provide and receive alternative payments that do not violate current sanction policies. Beyond direct exposure to the region, the war is likely to continue to raise key commodity prices and be a driver of inflation.

Supply chain risk

Ensure that organisations have updated supplier contingency plans in place that reflect the current environment. Supply chain risk should be freshly evaluated and efforts made to identify and limit any individual supplier dependency.

- **Learning Point:** Consider these four areas to reduce the threat to your institution from the ongoing war in Ukraine.

Organisations Need To Evolve Their Data Management Strategy

IDC predicts that, over the next five years, more than 80% of the data collected by organizations will be unstructured data, and that will only continue to grow 40-50% per year for most enterprises.

Main Article

Five main components of an effective data mobility engine

1. Vendor-neutral interoperability
There must be a focus on data, not systems, and be able to move data between different types of systems as well as cloud targets.

2. Insights and intelligence
Provide visibility into data metrics, access patterns, and usage activities that can provide the basis for classification, and this visibility must be comprehensive.

3. Orchestration and automation
Automation improves the speed and reliability of operations while improving administrative productivity, increasing the span of administrative control to lower costs.

4. Scan-optimize-copy capabilities
Scan provides the visibility around data and its usage, collecting the metrics needed to search and intelligently manage data.

5. Integrity enforcement
Support data integrity during all operations to be able to catch and correct silent data corruption using "before" and "after" hash digest comparisons, chain of custody, and advanced integrity protection.

Learning Points:
Something that should be looked at closely as the benefits of an effective data management strategy include reduced IT costs, easier data sharing, better security, less legal exposure, and an improved ability to demonstrate governance and regulatory compliance.

Lokilocker Ransomware Family Spotted With Built-In Wiper

BlackBerry security researchers have identified LokiLocker, a ransomware-as-a-service (RaaS) family targeting English-speaking victims that is capable of erasing all non-system files from Windows PCs.

Main Article Support Information

LokiLocker puts a time limit for paying the ransom and will make the system unusable if the payment isn't made. The malware also includes a wiper function that will erase the data if the payment deadline passes. It will delete files on all of the victim's drives, except for the system files, and it will also try to overwrite the Master Boot Record (MBR) of the system drive to render the system unusable.

The wiper function is part of an escalation by ransomware gangs in recent years to encourage victims to pay the ransom by including additional threats beyond just refusing to decrypt the files, such as erasing data or leaking stolen files on the dark web.

Learning Points:

- For cyber criminals this is a last resort as they try to monetize their attacks. Wipers are being seen in attacks against Ukraine, the driving motivation in cyber warfare is to disrupt, destroy and to instigate chaos.
- Ensure that you have backups and the capability to restore services from nothing.

All the best from all of us at **HEFESTIS** and look out for our next **Threatscape** update next week.

HEFESTIS Weekly Newsletter

A very warm welcome to all from the CISO-Share Office.

And thank you to all who attended the HEFESTIS Cyber Scotland Week sessions last week. The recordings are now available on our SharePoint site and will be soon linked from the Cyber Scotland Week website.

This week our thoughts remain with all of those facing war and oppression in Europe and across the globe.

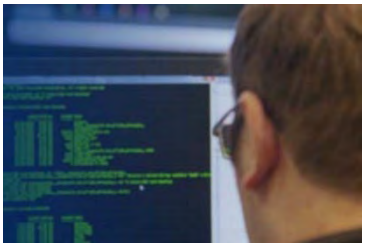
Please check the CiSP site, as always, for the latest updates on current incidents and countermeasures to protect your institution. Whilst you are here, why not drop into the CISO-Share user forum and discuss the latest topics and news.

We have just been notified of further malicious activity from Russian based IP addresses. We recommend blocking the following IPs and checking to see if there has been any malicious activity:

45.143.200.114
185.191.32.211
45.155.204.214
45.155.205.44
45.155.204.63
45.155.205.40
45.155.205.49
45.146.164.152
45.155.205.41
45.155.205.48

If you have any questions or comments, please feel free to contact us via CISO-Office@hefestis.ac.uk.

Here are some of the week's Cyber Security articles which caught the attention of CISO-Share.



New Scottish centre aims to boost cyber defences

https://dailybusinessgroup.co.uk/2022/02/new-scottish-centre-aims-to-boost-cyber-defences/

SC3 was announced ahead of the start of Cyber Scotland Week by the Deputy First Minister John Swinney.

Scotland's ability to prevent and respond to growing threats posed by hackers has been strengthened with the creation of a Cyber Co-ordination Centre (SC3).

The centre, backed by £1.5m from the Scottish government, will share intelligence, provide early warning of cyber threat and attacks, manage incidents and lead recovery.

The SC3 will have a primary focus on the public sector initially, and in its first year, will look at how Scotland can manage threat and vulnerability at scale; how to build the cyber security capabilities of the public sector and how responses to incidents can be more rapidly identified, managed and investigated.

Action Point:
An exciting time for the sector and the cyber security sector in Scotland. HEFESTIS is in partnership with the SC3 to ensure that our members are kept informed of progress, have a direct communication channel and can help to guide the work and priorities of the SC3.

PROUD SUPPORTER OF Cyber Scotland Week

Cyber Scotland Week 2022

Thanks to all those who attended the HEFESTIS Cyber Scotland Week sessions. These events were a joint effort between the HEFESTIS DPO-Share and CISO-Share services.

We hope that you found the sessions informative and helpful. The recorded content and material from the sessions are now available for access in the HEFESTIS CISO-Share SharePoint site for our members to access.

Cyber Scotland Week 2022

Public Sector Cyber Security Scotland 2022 - Holyrood Events

High threat areas

Organisational Approach to Cyber Security

Cyber attack identification and response

The Importance of Tabletop Cybersecurity Exercises

https://securityboulevard.com/2022/03/the-importance-of-tabletop-cybersecurity-exercises/

Tabletop exercises improve a teams' disaster preparedness, coordination skills and role/responsibility disruption under duress. And these exercises also help program managers identify deficiencies in cybersecurity process/procedures, personnel shortcomings and additional training requirements.

A tabletop exercise is a preparedness activity where participants are taken through a simulated security incident to highlight flaws and areas of improvement in their response planning. The primary goal is to evaluate a incident response plan and the response team's reaction to a cyberattack, reveal gaps in the incident response plan and practice responses without the risk of damaging or disrupting normal business processes.

Tabletop exercises will reduce the risk of damage from a cybersecurity attack, which gives organisations greater peace of mind and confidence that their experts can execute a recovery plan efficiently.

A third party or trusted partner can also give an unbiased assessment a company's current cybersecurity defences, readiness and resilience.

Action Point:
Schedule a TTX either internally or with your HEFESTIS CISO. This is also one of the recommendations for operation within a heightened alert situation.

Conti Ransomware - IOC update

https://www.cisa.gov/uscert/ncas/alerts/aa21-265a

March 9, 2022: this joint CSA was updated to include indicators of compromise (see below) and the United States Secret Service as a co-author. Thanks go out to Dundee and Angus college for raising awareness of this update.

Updated February 28, 2022:

Conti cyber threat actors remain active and reported Conti ransomware attacks against U.S. and international organizations have risen to more than 1,000. Notable attack vectors include Trickbot and Cobalt Strike (see below for details).

While there are no specific or credible cyber threats to the U.S. homeland at this time, CISA, FBI, and NSA encourage organizations to review this advisory and apply the recommended mitigations.
The Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) have observed the increased use of Conti ransomware in more than 400 attacks on U.S. and international organizations. (See FBI Flash: Conti Ransomware Attacks Impact Healthcare and First Responder Networks.) In typical Conti ransomware attacks, malicious cyber actors steal files, encrypt servers and workstations, and demand a ransom payment.

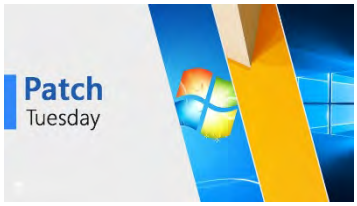
To secure systems against Conti ransomware, CISA, FBI, and the National Security Agency (NSA) recommend implementing the mitigation measures described in this Advisory, which include requiring multifactor authentication (MFA), implementing network segmentation, and keeping operating systems and software up to date.

Click here for a PDF version of this report.
Click here for indicators of compromise (IOCs) in STIX format.

Action Point:
The Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) have observed the increased use of Conti ransomware in more than 400 attacks on U.S. and international organizations. (See FBI Flash: Conti Ransomware Attacks Impact Healthcare and First Responder Networks.) In typical Conti ransomware attacks, malicious cyber actors steal files, encrypt servers and workstations, and demand a ransom payment.

To secure systems against Conti ransomware, CISA, FBI, and the National Security Agency (NSA) recommend implementing the mitigation measures described in this Advisory, which include requiring multifactor authentication (MFA), implementing network segmentation, and keeping operating systems and software up to date.

Click here for a PDF version of this report.
Click here for indicators of compromise (IOCs) in STIX format.



Patch Tuesday: Microsoft Fixes Multiple Code Execution Flaws

https://www.securityweek.com/patch-tuesday-microsoft-fixes-multiple-code-execution-flaws

Microsoft's Patch Tuesday bundle for this month is a big one: 74 documented vulnerabilities in multiple Windows products and components, some serious enough to lead to remote code execution attacks.

The Redmond, Wash.-based software giant cautioned that exploit code is publicly available for three of the patched vulnerabilities -- remote code execution bugs in Remote Desktop Client and .NET and Visual Studio, and a privilege escalation flaw in the Windows Fax and Scan service.

Action Point: Vulnerability trackers at the Zero Day Initiative are calling special attention to the Microsoft Exchange server flaw -- CVE-2022-23277 -- as one that needs to be tested and deployed with urgency.

Adobe Patches 'Critical' Security Flaws in Illustrator, After Effects

https://www.securityweek.com/adobe-patches-critical-security-flaws-illustrator-after-effects

Software maker Adobe on Tuesday shipped urgent security updates to fix code execution vulnerabilities in the widely deployed Illustrator and After Effects products.

The patches, scheduled as part of Adobe's Patch Tuesday release cycle, address a range of arbitrary code execution and memory leak vulnerabilities that could expose data to malicious hacker attacks. The most serious of the vulnerabilities was addressed in Adobe Illustrator, the popular vector graphics design program available for both macOS and Windows systems.

Action Point:
In an advisory, Adobe rated the Illustrator flaw as "critical" with a CVSS base score of 7.8. The company described the CVE-2022-23187 bug as a buffer overflow affecting Illustrator 2022 version 26.0.3 (and earlier versions) on both WIndows and macOS machines.
Adobe is strongly urging users to upgrade to Illustrator 2022 version 26.1.0.

New 16 High-Severity UEFI Firmware Flaws Discovered in Millions of HP Devices

https://thehackernews.com/2022/03/new-16-high-severity-uefi-firmware.html?m=1

Cybersecurity researchers on Tuesday disclosed 16 new high-severity vulnerabilities in various implementations of Unified Extensible Firmware Interface (UEFI) firmware impacting multiple HP enterprise devices.

The devices affected includes HP's laptops, desktops, point-of-sale (PoS) systems, and edge computing nodes.

The most severe of the flaws concern a number of memory corruption vulnerabilities in the System Management Mode (SMM) of the firmware, thereby enabling the execution of arbitrary code with the highest privileges.

Firmware has emerged as an ever-expanding attack surface for threat actors to launch highly-targeted devastating attacks. At least five different firmware malware strains have been detected in the wild to date since 2018.

Action Point:
Cyber Essentials requirements cover a devices firmware. To comply and attain certification there needs to be an update process in operation similar to other software patching. Ensure that there is a process and sufficient resource to meet the requirements for firmware updates.

Unpacking MITRE's new Engage cybersecurity framework

https://sectrio.com/unpacking-mitres-new-engage-cybersecurity-framework/

Mitre on Wednesday released a new communication and planning framework for cyber adversary engagement that focuses on deception and denial.
In the past year, MITRE ran a series of focus groups with vendors, defenders, and CISOs to solicit feedback and insight into Engage's development.

Here are some of the highlights of the new framework:

- It is essentially designed to shrink barriers to better cybersecurity planning and analysis by enabling the development of a coherent institutional anti-cyber adversarial strategy.
- Unlike frameworks that propose one barrier (often at the perimeter level), the Engage framework proposes blocking an intrusion as a first step and engaging and deceiving an adversary if they have managed to cross the entry threshold
- In this sense, the Engage framework is essentially proposing a multi-pronged strategy to protect enterprises
- It can help defenders identify a cyber adversary's weaknesses while using a specific ATT&CK technique. This weakness can then be used against the adversary to degrade the quality of attack
- It proposes to engage the adversary through deception operations to reduce the cost of a data breach, keep the attacker engaged in wasteful endeavors and make the attack easier to detect and target
- It is oriented towards making cyber adversaries fail early so that they are led into a decoy alley from which it will be hard for them to escape and strike back at core assets

- CISOs can use Engage to plan better, in-house cybersecurity teams can use it to deploy better protective measures while cybersecurity vendors can align their products to it to improve defense outcomes
- The Engage toolkit includes a guidebook, starter kit, worksheets, posters, and other resources designed to help improve the adoption of the framework
- The framework also standardizes technology terms to make it easier for cross-geography teams to collaborate. It is also designed to engage the relatively less experienced user as well

Action Point:
Cyber defenders, and vendors can learn more about Engage and get involved in the Engage community at https://engage.mitre.org/.

https://www.mitre.org/news/press-releases/mitre-launches-engage-framework-to-defend-against-cyber-attacks

---

Open Source Security Foundation (OpenSSF)

https://www.techrepublic.com/article/new-openssf-project-may-finally-be-doing-security-right/

The Open Source Security Foundation (OpenSSF) members help identify and fix security vulnerabilities in open source software and develop improved tooling, training, research, best practices and vulnerability disclosure practices.

OpenSSF also announced the Alpha-Omega Project, a project that attempts to identify all of the world's most critical, foundational open-source software libraries and packages and audit them and then support them as necessary.

"Alpha" will work with the maintainers of the most critical open source projects to help them identify and fix security vulnerabilities and improve their security posture. "Omega" will identify at least 10,000 widely deployed OSS projects where it can apply automated security analysis, scoring and remediation guidance to their open source maintainer communities."

Action Point:
Alpha-Omega is a great start to trying to resolve issues across the open source community. This will also help us manage the open source software and library in use at our organisations.

Researchers Warn of Linux Kernel 'Dirty Pipe' Arbitrary File Overwrite Vulnerability

https://thehackernews.com/2022/03/researchers-warn-of-linux-kernel-dirty.html

Dirty Pipe Vulnerability

Linux distributions are in the process of issuing patches to address a newly disclosed security vulnerability in the kernel that could allow an attacker to overwrite arbitrary data into any read-only files and allow for a complete takeover of affected systems.

Dubbed "Dirty Pipe" (CVE-2022-0847, CVSS score: 7.8) by IONOS software developer Max Kellermann, the flaw "leads to privilege escalation because unprivileged processes can inject code into root processes."

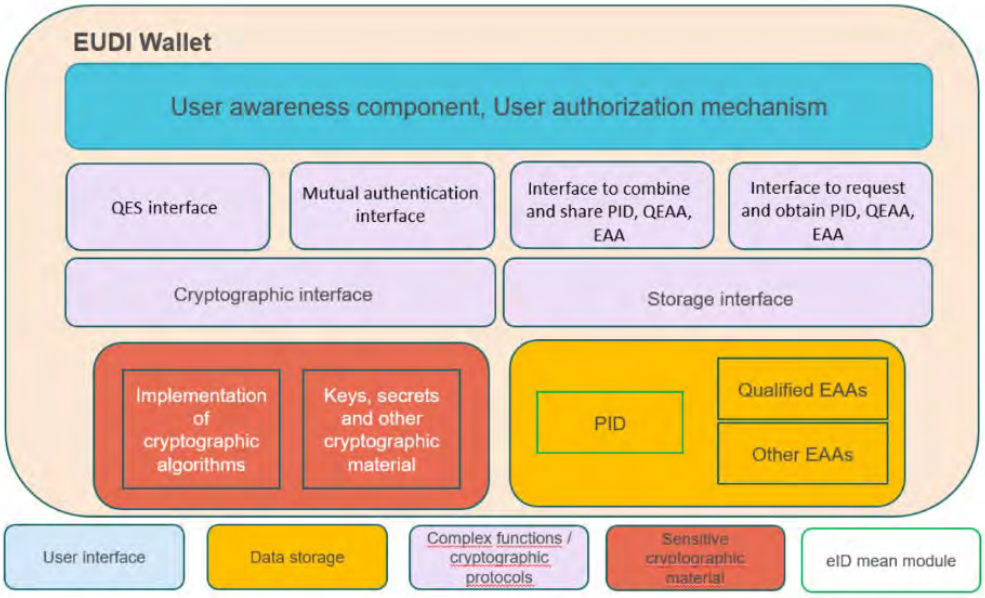
Kellerman said the bug was discovered after digging into a support issue raised by one of the customers of the cloud and hosting provider that concerned a case of a "surprising kind of corruption" affecting web server access logs.

Action Point:
The issue has been fixed in Linux versions 5.16.11, 5.15.25, and 5.10.102 as of February 23, 2022, three days after it was reported to the Linux kernel security team. Google, for its part, has merged the fixes into the Android kernel on February 24, 2022.

Given the ease with which the security flaw can be exploited and the release of the PoC exploit, it's recommended that users update Linux servers immediately and apply the patches for other distros as soon as they are available.

EU digital identity architecture and reference framework

https://blog.avast.com/analysis-of-eu-digital-identity-architecture-and-reference-framework-avast



The European Digital Identity Architecture and Reference Framework (the "Framework") points to a focused and deliberate drive towards secure digital identity for all European citizens and sets the standard for the rest of the world.

Overview of the EUDI Wallet roles.

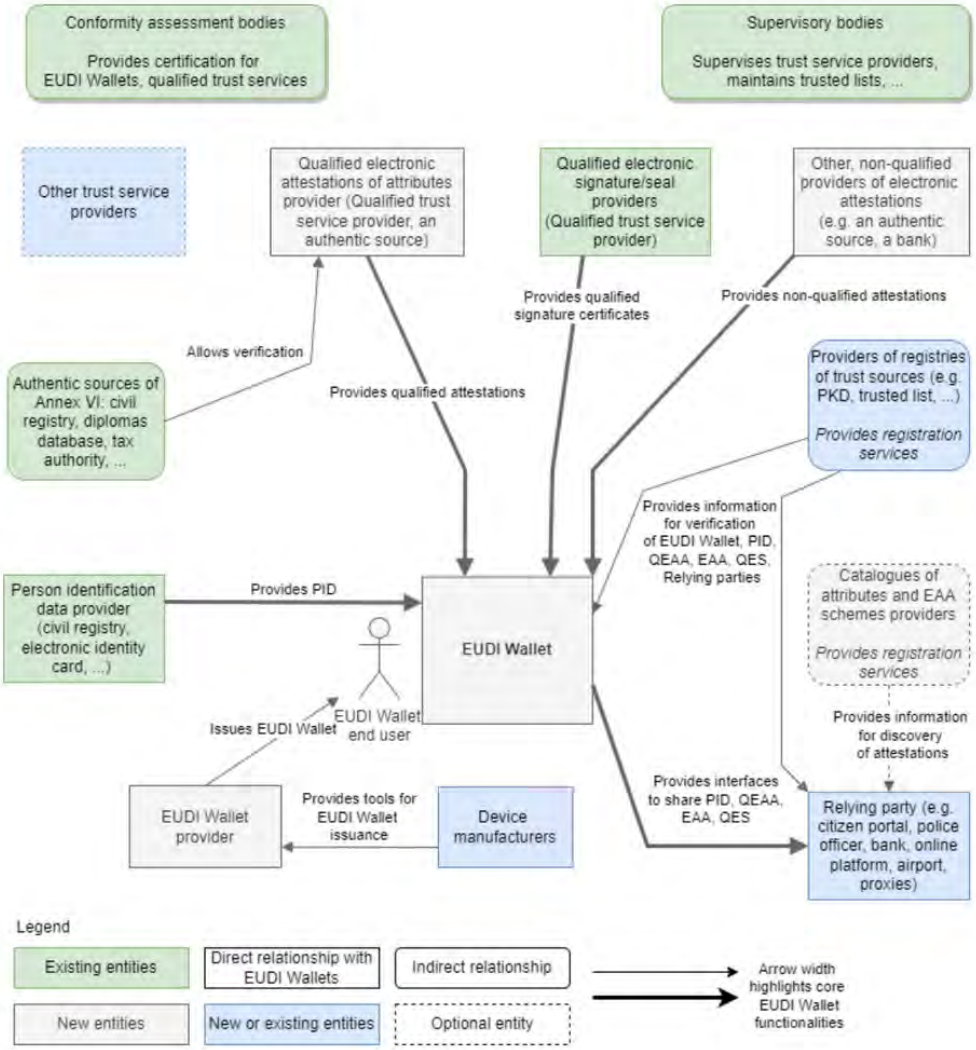


Figure 1 Overview of the EUDI Wallet roles

Interesting to see a digital government identification standard for the EU that can also be used for non-government bodies. This could well be the start of a single digital identity for EU citizens which is used for all digital identification.

This article provides analysis of the framework and looks at the good and the bad within the proposal.

Action Point:
Although no longer in the EU, this is an interesting framework and one to keep an eye on as it is a proposal which could find its way into the UK as a standard digital identification.

2 New Mozilla Firefox 0-Day Bugs Under Active Attack

https://thehackernews.com/2022/03/2-new-mozilla-firefox-0-day-bugs-under.html

Mozilla has pushed out-of-band software updates to its Firefox web browser to contain two high-impact security vulnerabilities, CVE-2022-26485 and CVE-2022-26486, both of which it says are being actively exploited in the wild.

The description of the two flaws is below:

- **CVE-2022-26485** – Removing an XSLT parameter during processing could lead to an exploitable use-after-free
- **CVE-2022-26486** – An unexpected message in the WebGPU IPC framework could lead to a use-after-free and exploitable sandbox escape

Action Point:
Users are recommended to upgrade as soon as possible to Firefox 97.0.2, Firefox ESR 91.6.1, Firefox for Android 97.3.0, Focus 97.3.0, and Thunderbird 91.6.2.

All the best from all of us at **HEFESTIS** and look out for our next **Threatscape** update next week.

HEFESTIS Weekly Newsletter

A very warm welcome to all of you from all of us at the CISO-Share Office.

Thank you all for your responses to yesterday's alert about port 554 suspicious activity. Although a related incident was reported in the wider public sector, your prompt action has potentially helped maintain our record of no significant breaches being recorded over February and early March 2022 from the HE/FE sector in Scotland.

From next week we are introducing a new CISO-Office mailbox. CISO-Office@hefestis.ac.uk.

The new mailbox has been added to improve our membership communications. All messages posted to the new address will be directed to and triaged by all of your CISO's to ensure a rapid response. Use of the CISO-Office@hefestis.ac.uk account is intended to improve our service resilience, support incident response queries and urgent correspondence. The new account has been introduced so that members who need to communicate with us for IR (threats, alerts, strange notifications) purposes have a single channel of contact.

Our response process therefore changes from direct contact as individuals to shared contact with the team. The channel can also be used for general queries should your shared CISO be unavailable. We hope this small change will make it easier to engage with the CISO-Share Office.

This week our thoughts remain with all of those facing war and oppression in Europe and across the globe.

Please check the CiSP site, as always, for the latest updates on current incidents and countermeasures to protect your institution.

Whilst you are here, why not drop into the CISO-Share user forum and discuss the latest topics and news.

Just a reminder that we have completed our migration to SharePoint and hope you are enjoying the richer experience. There have been no issues reported for quite some time now and we are happy to announce that the Teams site content, hosted by University of Dundee, is now well established in our library section. With the new forum open within the CiSP secure site, the teams site has been retired after 4 months of inactivity. We would like to thank the staff at University of Dundee for supporting our members by hosting the site for 2 years.

Cyber Scotland week has been a great engagement for us all with the final sessions, including our last webinar concluding today. Thanks to all who attended and supported our activity over the course of this week – it was also great to meet some of you in person at Dynamic Earth on Tuesday.

We would like to thank John Maher in particular for giving an outstanding and insightful talk on the lessons learned from incident response at UHI. The session was strongly attended by our membership and greatly appreciated.

This week we cover the rising level and evolving profile of cyber security threats we face.

Ukraine situation - cyber security information from NCSC.

There is an abundance of news and information constantly streaming relating to the ever changing and conflictual situation in Ukraine, however we have no actionable intelligence demonstrating the HE/FE sector in the UK is showing any signs of being **specifically** targeted by any related cyber-attacks at this time.

If we hear of anything specific, we will let everyone know immediately. At time of going to press, the existing guidance from NCSC still applies.

Our colleagues at the National Cyber Security Centre (NCSC), the UK's technical authority on cyber security, have issued guidance for organisations on the steps they need to take to bolster the UK's resilience against the heightened risk of malicious cyber incidents in and around Ukraine. We know many organisations and businesses in the UK have well laid out plans and good cyber security measures in place. However due to the nature of online global networks, attacks that occur overseas could have an impact on UK institutions, services and systems. This is why organisations and businesses are being urged to take action now.

While the NCSC is not aware of any current specific threats to UK organisations in relation to events in and around Ukraine, the guidance encourages organisations to follow actionable steps that reduce the risk of being impacted by cyber-attacks, including:

- patching systems;
- improving access controls and enabling multi-factor authentication;
- implementing an effective incident response plan;
- checking that backups and restore mechanisms are working;
- ensuring that online defences are working as expected, and;
- keeping up to date with the latest threat and mitigation information.

For further information visit: https://www.ncsc.gov.uk/guidance/actions-to-take-when-the-cyber-threat-is-heightened where you will find the relevant advice, actions and resources.

We would also encourage you to follow the NCSC's social media channels: LinkedIn and Twitter for further alerts and updates.

If you have any questions, please contact enquiries@ncsc.gov.uk or the CISO-Share team who will be happy to assist.

List Of Data Breaches And Cyber Attacks In February 2022 – 5.1 Million Records Breached

The cyber security industry, much like the rest of the world, is on edge. Our figures for this month are comparatively low – with 83 data breaches and cyber-attacks accounting for 5,127,241 breached records – but there is a sense that we are on the brink of something.

Main Article

In the final days of February, there were a flurry of security incidents related, either directly or indirectly, to the Ukraine conflict. First, Russia targeted banks and government departments, then Ukraine hit back, attacking the Moscow stock exchange.

The EU has responded to calls for help from Ukraine and has set up a cyber rapid-response team comprised of 12 volunteers, who will help cyber-attack victims. The hacking group Anonymous has been more aggressive, launching attacks across Europe to give Vladimir Putin "a sip of his own bitter medicine".

In the midst of all this, organisations across Europe have reported delays as a result of alleged state-sponsored attacks – including Toyota's Japanese plants and a kettle manufacturer in the Isle of Man.

Action Point: You can find the full list of cyber-attacks and data breaches for February 2022 here. As usual, incidents affecting UK-based organisations are listed in bold.

Log4Shell: Still Out There, Still Dangerous, And How To Protect Your Systems

Barracuda researchers have noticed a steady stream of attacks attempting to exploit the Log4j vulnerability since it was found. What's interesting is where most attacks originate.

Main Article

Log4Shell, an exploit directed at the commonly used Apache Log4j library, hasn't shown any signs of slowing down as a popular target for hackers since its discovery in December, said researchers at Barracuda Networks.

Log4Shell is just about as critical as a critical vulnerability can get. It scored 10 out of 10 by the National Institute of Standards and Technology's severity scale, and with good reason: It targets a library that nearly every Java application uses to log requests, and all it takes to trigger it is a malicious string from the attacker.

Since its discovery in December, said Barracuda Senior Product Marketing Manager for Applications and Cloud Security Tushar Richabadas, "the volume of attacks attempting to exploit these vulnerabilities has remained relatively constant with a few dips and spikes over the past two months."

83% of the attacks that have tried the exploit Log4Shell originated in the United States.

Action Points: Easier said than done but -

There's a simple fix that could completely remove this risk from your cybersecurity calculus: Patch to the latest version of Log4j, which takes care of the problem.

That isn't always possible in production environments, so if you're unable to patch now there are steps you can take to determine if your systems are vulnerable to Log4Shell, as well as different things that can be done to minimize your Log4Shell exposure … until you can actually install the patch, which should be your eventual goal.

Security Challenges Hampering Organisations In Achieving Their Security Objectives

Arctic Wolf published a report, providing insight into the current and future state of cybersecurity teams.

Main Article

Persistent weaknesses trump novel attack methods as top security concerns

70% have existing latent threats

81% rated vulnerabilities and unknown misconfigurations as the biggest security concerns within their environments

50% say their security budget in 2022 is lacking in a way that will not let them achieve their security objectives

30% with cyber insurance who were surveyed say their policy costs went up or were cancelled outright in 2021, while 35% currently operate without any form of cyber insurance.

The Great Resignation widens the cybersecurity skills gap

84% have not been able to fulfil their target headcounts regarding security staff

76% say that their primary obstacle for achieving their cybersecurity objectives is either the struggle to hire staff or the lack of expertise within current staff

44% do not have any staff members assigned to security as their fulltime or primary function.

Cloud adoption is outpacing cloud security

47% of all incidents investigated include at least one cloud component

Only 19% dare using cloud security posture management (CSPM) as a way of securing their cloud resources

22% currently have plans in place to add it to their security program.

Action Points:

Organisations that can rely on a mature security operations practice in 2022 will find themselves more secure, more resilient, and better able to adapt to the multitude of internal and external risk factors.

Continue to progress the pathway and take a risk-based approach to maturity prioritisation.

New Security Vulnerability Affects Thousands of GitLab Instances

Tracked as CVE-2021-4191 (CVSS score: 5.3), the medium-severity flaw affects all versions of GitLab Community Edition and Enterprise Edition starting from 13.0 and all versions starting from 14.4 and prior to 14.8.

Main Article

A remote, unauthenticated attacker can use this vulnerability to collect registered GitLab usernames, names, and email addresses.

Successful exploitation of the API information leak could permit malicious actors to enumerate and compile lists of legitimate usernames belonging to a target that can then be utilized as a steppingstone to conduct brute-force attacks.

Besides CVE-2021-4191, the patch also addresses six other security flaws, one of which is a critical issue (CVE-2022-0735, CVSS score: 9.6) that enables an unauthorized attacker to siphon the runner registration tokens used to authenticate and authorize CI/CD jobs hosted on GitLab instances.

Action Points:

- If you use GitLab as part of your DevOps processes then ensure that it is kept up to date.

Partner Event: Cyber Security Procurement Support Tool for Public Sector Suppliers

Cyber Resilience - helping you meet the requirements of public sector tendering

Cyber Security Procurement Support Tool for Suppliers

Thursday 14 April 2022, 10.30am-12:00pm

We have received this event notification from the cyber resilience unit which may be of interest for those of you considering using the Cyber Security Procurement Support Tool for Suppliers. The session should cover any questions you might have around use of the tool. (You may have to register for use of the tool here first https://cyberassessment.gov.scot/)

Here is the invite link. https://www.sdpscotland.co.uk/events/cyber-resilience-helping-you-meet-the-requirements-of-public-sector-tendering-1238/.

- **Learning Point:** The Scottish public sector is being encouraged to ensure its suppliers have appropriate cyber security in place. In this climate of ever-increasing cyber threat, supply chains are often seen as an easy route to attack larger organisations.

---

100 Million Samsung Galaxy Phones Affected with Flawed Hardware Encryption Feature

A group of academics from Tel Aviv University have disclosed details of now-patched "severe" design flaws affecting about 100 million Android-based Samsung smartphones that could have resulted in the extraction of secret cryptographic keys.

Main Article

The shortcomings are the result of an analysis of the cryptographic design and implementation of Android's hardware-backed Keystore in Samsung's Galaxy S8, S9, S10, S20, and S21 flagship devices, researchers Alon Shakevsky, Eyal Ronen, and Avishai Wool said.

Trusted Execution Environments (TEEs) are a secure zone that provide an isolated environment for the execution of Trusted Applications (TAs) to carry out security critical tasks to ensure confidentiality and integrity.

Learning Points: Please remember, we also have to patch our mobile devices.

Following responsible disclosure in May and July 2021, the issues were addressed via security updates shipped in August and October 2021 for the affected devices. The findings are expected to be presented at the USENIX Security Symposium later this August.

Cyberattacks in Ukraine: New Worm-Spreading Data-Wiper With Ransomware Smokescreen

Cybersecurity researchers tracking destructive data-wiping malware attacks in Ukraine are finding signs of new malware with worm-spreading capabilities and what appears to be a rudimentary ransomware decoy.

Main Article

IOC's from CISA

According to new research from Slovakian anti-malware company ESET, the cyberattacks began hours before Russia's invasion of Ukraine on February 24 with DDoS attacks against Ukrainian government websites and quickly morphed into wiper attacks aimed at destroying data on computer networks.

In all, ESET found the initial attacks leveraging three components:

HermeticWiper makes a system inoperable by corrupting its data

HermeticWizard spreads the data-wiper like a computer worm across a local network via WMI and SMB

HermeticRansom adds a data-extortion ransomware component written in Go.

Learning Points:

- The U.S. government's cybersecurity agency CISA has released indicators of compromise to help threat hunters look for signs of the data-wiping threats in computer networks.

All the best from all of us at **HEFESTIS** and look out for our next **Threatscape** update next week.

HEFESTIS Weekly Newsletter

A very warm welcome from all of us at the CISO-Share Office.

This week we cover the rising threat due to the Ukraine Crisis, the adoption of a "Just Culture", free tools and best practice.

Please check the CiSP site, as always, for the latest updates on current incidents and countermeasures to protect your institution.
Whilst you are there, why not drop into the CISO-Share user forum and discuss the latest topics and news.

Our events, most of which are open to all, are up on the CSW2022 website - and can be accessed either through our SharePoint site or by following this link.
https://events.cyberscotlandweek.com/events/?tribe_paged=1&tribe_event_display=list&tribe-bar-date=2022-02-16&tribe-bar-search=hefestis

And don't forget David will be joining the Holyrood Communications' forthcoming Public Sector Cyber Security Scotland 2022 event. David will be presenting on how we are all working together to address the cyber challenges facing the HE/FE community in Scotland.
You can view the event's full agenda here:
https://events.holyrood.com/event/public-sector-cyber-security-scotland-2022/

If you have any questions or comments, please feel free to contact us.

Steve McIntosh
M: 07904 908945
E: smcintosh@hefestis.ac.uk

David Robertson
M: 07852 330122
E: drobertson@hefestis.ac.uk

Darren Clement
M: 07442 859979
E: dclement@hefestis.ac.uk

Here are some of the week's Cyber Security articles which caught the attention of CISO-Share.

Cyberwarfare Risks Continue as Ukraine Crisis Escalates

https://securityboulevard.com/2022/02/cyberwarfare-risks-continue-as-ukraine-crisis-escalates/

Cybersecurity experts continue to sound the alarm as Russia's invasion of Ukraine intensifies and fears of global cyberwarfare that could have wide-ranging impacts on governments and organisations of all sizes grow.

CISA published its Preparing for and Mitigating Foreign Influence Operations Targeting Critical Infrastructure advisory, which provided critical infrastructure owners and operators with guidance for identifying and mitigating the risks of influence operations that use mis-, dis-, and malinformation (MDM) narratives.

Much of the immediate concern is focused on a flurry of malicious activity targeted at Ukrainian organizations prior to Russia's military action. This includes the deployment of a dangerous new disk-wiping malware tool, crippling DDoS attacks, and a new malware framework from a Russian threat actor tied to the Russian General Staff Main Intelligence Directorate (GRU).

Earlier this month, CISA urged US organisations to assume what it calls a "Shields Up" stance in preparation for cyberattacks by Russia-backed threat actors.

Following Russia's further violation of Ukraine's territorial integrity, the National Cyber Security Centre has called on organisations in the UK to bolster their online defences.

Action Point:
While the NCSC is not aware of any current specific threats to UK, we need to be able to detect and investigate as quickly as possible to make sure that we aren't used by Russia as part of their military exploits.

- https://www.ncsc.gov.uk/news/organisations-urged-to-bolster-defences
- https://www.darkreading.com/attacks-breaches/fears-rise-of-potential-russian-cyberattacks-on-us-allies-over-sanctions

---

How Instituting a 'Just Culture' Improves Security

https://www.darkreading.com/edge-articles/how-instituting-a-just-culture-improves-security

Trust, accountability, and ongoing improvement serve as the foundation for just culture. The concept has its origins in the aviation industry, though it has caught on in healthcare and many other fields.

Just culture isn't about eliminating responsibility. It also doesn't attempt to sugarcoat glitches and breakdowns. It emphasizes accountability by asking, "*What went wrong?*" rather than, *"Who caused the problem?"*

Within cybersecurity, for example, just culture might translate into rethinking software and workflows to avoid shadow IT, putting protocols such as strong identity and access management (IAM) and multifactor authentication (MFA) in place to avoid authentication failures, and adopting protocols such as 802.1x to better control and manage network access, including wireless devices. The success of a just culture initiative also hinges on the words and actions of the executive suite, there a need to establish formal reporting mechanisms, including the ability for people to remain anonymous.

What makes just culture so powerful is that people feel free to point out errors and problems.

Action Point:

If not already in place introduce a no blame "Just Culture" at your organisation.

Attackers use Microsoft Teams as launchpad for malware

https://www.helpnetsecurity.com/2022/02/17/microsoft-teams-malware/

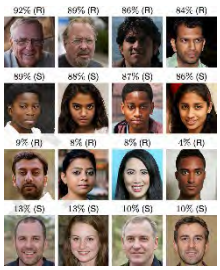
Hackers are starting to realize that Microsoft Teams is a great means of spreading throughout an organization's systems. This specific attack involves attackers compromising an account and attaching .exe files to Teams chats.

Scanning for malicious links and files is limited in Microsoft Teams, and many third-party security solutions are not that great when it comes to Teams-specific protection.

In addition to this, while most employees have by now learned to second-guess identities in email, they still have an inherent trust in the identities on Teams.

Action Point:

Be aware of attack evolutions and ensure that the same security principles are applied to all communication services.



AI-created faces now look so real, humans can't spot the difference

https://www.theregister.com/2022/02/21/ai_created_faces_fool_humans/

Humans can no longer reliably tell the difference between a real human face and an image of a face generated by artificial intelligence, according to a pair of researchers.

In one part of the study – published in the Proceedings of the National Academy of Sciences USA – humans identified fake images on just 48.2 per cent of occasions.

The scientists said that while creating realistic faces is a success, it also creates potential problems such as non-consensual intimate imagery (often misnamed as "revenge porn"), fraud, and disinformation campaigns as nefarious use cases of fake images. Such activities, they wrote, have "serious implications for individuals, societies, and democracies."

There are currently ongoing efforts to improve detection of deepfakes and similar media, such as building prototype software capable of detecting generated images.

Action Point:

The point where deepfakes can be used in more complicated and successful attacks is drawing nearer. We need to be prepared to address any misinformation by ensuring that our communication channels are well defined and understood. Build up awareness of these channels and ensure that they are well protected.

Cybersecurity best practices for public and private organizations

https://www.helpnetsecurity.com/2022/02/21/eu-cybersecurity-best-practices/

The European Union Agency for Cybersecurity (ENISA) and CERT-EU published a joint set of cybersecurity best practices for public and private organizations in the EU.
An analysis of the rise in major threats is made available in the Agency's 2021 Annual Threat Landscape report.

- Ransomware remains a prime threat, putting millions of organizations at risk.
- Cybercriminals are increasingly motivated by the monetisation of their activities.
- Attacks against critical infrastructure are rising exponentially and other economical sectors as well as society at large can be exposed.

Action Point:
We strongly encourage all organisations to adopt a minimum set of cybersecurity best practices. You can see the ENISA recommendations from the following links, review and see if there are any gaps highlighted in your current approach.

FREE CYBERSECURITY SERVICES AND TOOLS

https://www.cisa.gov/free-cybersecurity-services-and-tools

As part of a continuing mission to reduce cybersecurity risk across U.S. critical infrastructure partners and state, local, tribal, and territorial governments, CISA has compiled a list of free cybersecurity tools and services to help organizations further advance their security capabilities.

This living repository includes cybersecurity services provided by CISA, widely used open-source tools, and free tools and services offered by private and public sector organizations across the cybersecurity community. CISA will implement a process for organizations to submit additional free tools and services for inclusion on this list in the future.

Action Point: All organizations should take certain foundational measures to implement a strong cybersecurity program

---

Local Authority Sets Aside £380k for Cyber-Attack Recovery

https://www.infosecurity-magazine.com/news/local-authority-380k-cyber-recovery

A local authority in the UK hit by suspected Russian actors has set aside £380,000 ($514,000) to remediate and recover from the incident, according to reports.

Gloucester City Council discovered the breach back in December and warned at the time that it could take up to six months to fix as servers would need rebuilding.
However, even the six-figure sum reserved to handle the fall-out of the incident may not be enough, councillors have admitted.

Action Point:

The Gloucester attack has been blamed on Russian attackers. Following a phishing email, “sleeper” malware was reportedly activated, although the end goal is still unclear.

HEFESTIS Cyber Scotland Week 2022

HEFESTIS are involved in and hosting a number of sessions over the Cyber Scotland Week 2022. The details of these sessions are below, along with the registration links for each of them. There will be a Q&A section at the end of each of the talks.

Cyber Resilience in a Post-Pandemic Public Sector

Tuesday 1st March 2022
10:00-11:15
Public Sector Cyber Security Scotland 2022 event

Speakers

David Robertson, CISO-Share
Description
This will involve a 15-minute presentation alongside two other speakers including Ivan McKee, Minister for Business, Trade, Tourism and Enterprise at the Scottish Government, as well as a collective Q&A.

https://events.holyrood.com/event/public-sector-cyber-security-scotland-2022/

Cyber-attack identification and response

Thursday 3rd March 2022
13:00-14:30
Open to all

Speakers

Jacqueline Gillanders, DPO-Share
Steven McIntosh, CISO-Share
David Robertson, CISO-Share

Description

This session has 3 talks.
The first from the HEFESTIS CISO Share Office and the Data Protection Office explains how to identify when you have been attacked.
The second also from the HEFESTIS CISO Share Office and the Data Protection Office then continues this discussion on how best to respond to an attack.
The third promotes the power of community and the benefits that come from a collaborative and collective approach.

Registration Link

https://teams.microsoft.com/registration/8J1YcZ1aLEiqfmGouScI7Q,PNe_g4syvUyZBpgWBbIHMg,jehmZFfy8EW-QpIH5gy-pw,8sC8TQIqIkiuGQPl6dfxpA,kGQG3iRNMkykqJdgjQAfpQ,9znfHhSfZ0eEnB53hDh7ag?mode=read&tenantId=71589df0-5a9d-482c-aa7e-61a8b92708ed

A Members experience of a major incident

Thursday 3rd March 2022
14:45-15:15
Closed Member Session

Description

We are extremely pleased and very grateful for the opportunity to hear and learn from one of our members of their experiences in dealing with an organisational major incident.
This is a member only session.

Registration Link

https://teams.microsoft.com/registration/8J1YcZ1aLEiqfmGouScI7Q,PNe_g4syvUyZBpgWBbIHMg,jehmZFfy8EW-QpIH5gy-pw,7FMckrEt1EmkSgvNHoqYxA,kX61y2yHSUqJ71Fn_N8BfQ,WGoTOpkNCEmNN8zxTCwMXQ?mode=read&tenantId=71589df0-5a9d-482c-aa7e-61a8b92708ed

Organisational Approach to Cyber Security

Thursday 3rd March 2022
15:30-16:30
Open to all

Speakers
Steven McIntosh, CISO-Share
David Robertson, CISO-Share

Description
This session is split into 2 HEFESTIS talks.

The first explains what HEFESTIS have learned about organisational security structures from their experience working across the HE/FE sector in Scotland.

The second gives an overview of the HEFESTIS cyber approach which has been developed to meet the needs of HEFESTIS member organisations and systematically progress their cyber maturity and risk management practices.

Registration Link
https://teams.microsoft.com/registration/8J1YcZ1aLEiqfmGouScI7Q,PNe_g4syvUyZBpgWBbIHMg,jehmZFfy8EW-QpIH5gy-pw,aMBfDcA56UG3QLFTGguuPQ,2VjsS5ABPEyndOn70kjvnQ,glSugdDg8UCUsRCOyres3g?mode=read&tenantId=71589df0-5a9d-482c-aa7e-61a8b92708ed

High threat areas
Friday 4th March 2022
13:00-14:30
Open to all

Speakers
James Nock, DPO-Share
Steven McIntosh, CISO-Share
Donald MacLean, DPO-Share
David Robertson, CISO-Share

Description
Fridays HEFESTIS session has 3 talks.
The first from the HEFESTIS CISO Share Office and the Data Protection Office explores supplier security.
The second talks about the steps that organisation can take to prepare for a ransomware attack.
The third looks at horizon scanning of current trends, and likely developments short to medium term.

Registration Link
https://teams.microsoft.com/registration/8J1YcZ1aLEiqfmGouScI7Q,PNe_g4syvUyZBpgWBbIHMg,jehmZFfy8EW-QpIH5gy-pw,9DeqSYJz8kq852JJ9EUBdg,QlXWWFKiyEi5F9Zxj5EQfQ,MCfSbNN7NkuRyhTqhgf1-A?mode=read&tenantId=71589df0-5a9d-482c-aa7e-61a8b92708ed

All the best from all of us at **HEFESTIS** and look out for our next **Threatscape** update next week.

HEFESTIS Weekly Newsletter

Good morning and a very warm welcome to all of you from all of us at the Ciso Share Office.

Positive news again as no significant breaches are reported over January 2022 from the HE/FE sector in Scotland.

This week we cover the latest Microsoft security patching, with some vulnerabilities already identified. We not only look back at 2021 but also forward to trends in 2022.

Please check the CiSP site, as always, for the latest updates on current incidents and countermeasures to protect your institution.

Whilst you are here, why not drop into the CISO-Share user forum and discuss the latest topics and news. Log into CiSP and head for the HEFESTIS CISO Share group. If any members do not have access yet, just click the following link and ask to join, we will let you in as soon as we can.

https://share.cisp.org.uk/groups/hefestis-ciso-share

Front and centre, Cyber Scotland week is getting closer, with the usual mix of interesting and informative sessions from across the public sector - including our good selves. Hope you can join in.

Here are a few of the articles which caught the attention of the CISO-Share team this week.

Cyber Scotland Week 28th February - 6th March 2022

This year's theme is "Learning for life online."

Keeping everyone cyber aware and resilient.

Main Website

As always, a good idea to keep this event in the diary and attend the events which interest or have value for you.

This year HEFESTIS will be hosting a number of events presented by the CISO-Share Office collaborating with our DPO-share service to bring a wider view of cyber-security to the event.

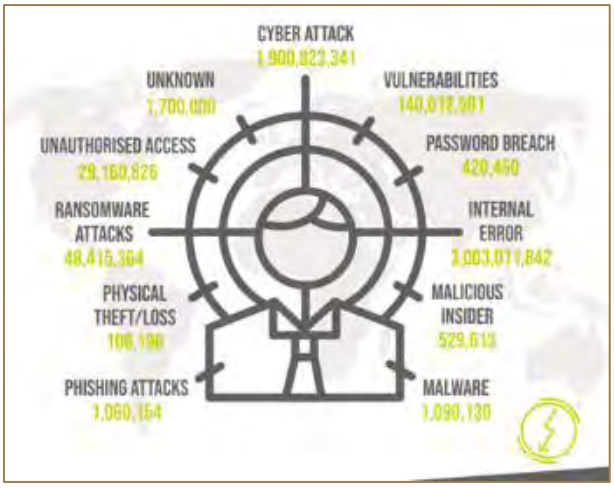
Sessions are planned on **Monday 28th February** plus **Thursday 3rd and Friday 4th March.** The details of each event covering different topical themes will be published here first so watch this space!

There is also an exciting opportunity to join the Holyrood Communications' forthcoming **Public Sector Cyber Security Scotland 2022 event** which is part of the conference. The event is taking place **in-person** in central Edinburgh on **1st March, 2022**. David from CISO Share will be speaking at the opening session entitled **Cyber Resilience in a Post-Pandemic Public Sector** taking place from **10:00 to 11:15**.

This will involve a 15-minute presentation alongside two other speakers including Ivan McKee, Minister for Business, Trade, Tourism and Enterprise at the Scottish Government, as well as a collective Q&A.

Looking forward to a great conference this year. Hope you can join us.

Action Point: Check the events calendar and reserve time in your diaries now.



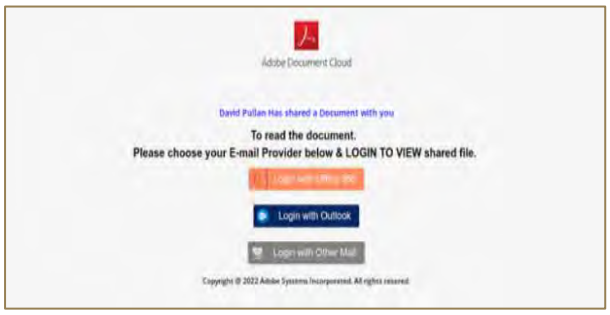
List of data breaches and cyber attacks in January 2022 – 66 million records breached

If there was any belief that 2022 would see a sudden improvement in the cyber security landscape, our first list data breaches and cyber attacks of the year should end that hope.

IT Governance discovered 95 security incidents in January, resulting in 65,984,648 compromised records.

You can find the full list of data breaches within the **Main Article** with incidents affecting UK organisations listed in bold.

Action Points:
Meanwhile, you might also be interested in the IT Governance **2021 data breach infographic**, which summarises the information from 12 monthly reports and reviews the year's key statistics.



Phishing Links In LinkedIn

Phishers can take advantage of a marketing feature which lets them create a LinkedIn.com link that bounces your browser to other websites, such as phishing pages that mimic top online brands (but chiefly Linkedin's parent firm Microsoft). This is not new with the issue first being highlighted in 2016.

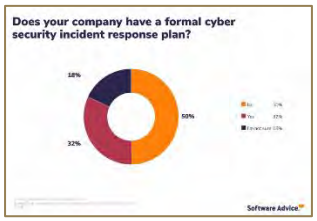
Main Article

A recent phishing site that abused LinkedIn's marketing redirect. Image: Urlscan.io.

Malicious or phishing emails that leverage LinkedIn's Slinks are unlikely to be blocked by anti-spam or anti-malware filters, because LinkedIn is widely considered a trusted domain, and the redirect obscures the link's ultimate destination.

Action Points:

- Advice to avoid phishing scams i.e., avoid clicking on links that arrive unbidden in emails, text messages and other mediums should be communicated to users. Most phishing scams warn of dire consequences should the recipient fail to respond or act quickly.
- Users should know how to report suspicious emails or if they have fallen victim to one.



UK organisations have experienced a 62% increase in cyber threats since 2020

Since the early days of the pandemic, experts warned that cyber criminals would thrive on new vulnerabilities and unfamiliar working conditions. However, few would have expected just how severe the threat would be.

Main Article

A Software Advice report has found that 62% of UK-based SMEs experienced an increase in cyber threats in the last two years.

Cyber attackers were most likely to target organisations with phishing emails, with 57% of incidents involving scam messages. Malware was another common threat and was found in 54% of cyber attacks.

- **Learning Point:** According to the study, 48% of executive managers said that employees had received no cyber security training in the last two years. Meanwhile, 32% said they didn't have a cyber security programme within their organisation and only half of organisations have a formal cyber security incident response plan.

Forensics as a Service (FaaS)

Digital forensics is a discipline that deals with the collection and analysis of systemic data and evidence after an incident or data breach has occurred in an organisation. The rapid adoption of Cloud Computing and remote working environment due to the pandemic has given rise to Forensics as A Service (FAAS).

Main Article

Many Cloud vendors have policies that state that they are not willing to provide file logs to subscribers. Additionally, cloud services can host a victim's data across multiple data centres, countries, and jurisdictions, which further adds to the complexity of challenges faced by investigators.

A typical FAAS involves the below steps:

- Initial Assessment
- Digital Evidence Acquisition & Recovery
- Forensic Examination and Analysis
- Forensics Reporting

Learning Points:
Consider how you would perform forensic investigations, including cloud based forensics, either internally or whether an external company would be necessary. Investigate these options and include them in incident response plans.

Kaspersky stopped more than 30,000 attempts to use the Log4Shell exploit in January

The critical remote code execution vulnerability in Apache's Log4j utility continues to be a popular tactic for cybercriminals. Consider this yet another plea to patch your systems.

Main Article

Cybersecurity company Kaspersky said it logged and blocked 30,562 attempts by hackers to use the Log4Shell exploit that was discovered in December 2021. While that marks a decline from when it was first reported, Kaspersky warns that it's here to stay as a new tool in cyber criminals' arsenals.

Learning Points:
Since the announcement of Log4Shell in December, Kaspersky said its products detected and prevented 154,098 attempts to scan and attack vulnerable devices, with most targets located in Russia, Brazil and the United States.

New Samba Bug Allows Remote Attackers to Execute Arbitrary Code as Root

Main Article

Samba has issued software updates to address multiple security vulnerabilities that, if successfully exploited, could allow remote attackers to execute arbitrary code with the highest privileges on affected installations.

CVE-2021-44142, rated 9.9 on the CVSS scale, impacts all versions of Samba before 4.13.17 and concerns an out-of-bounds heap read/write vulnerability in the VFS module "vfs_fruit" that provides compatibility with Apple SMB clients.

The flaw also affects widely used Linux distributions such as Red Hat, SUSE Linux, and Ubuntu.

Action Points:

- Samba administrators are recommended to upgrade to these releases or apply the patch as soon as possible to mitigate the defect and thwart any potential attacks exploiting the vulnerability.

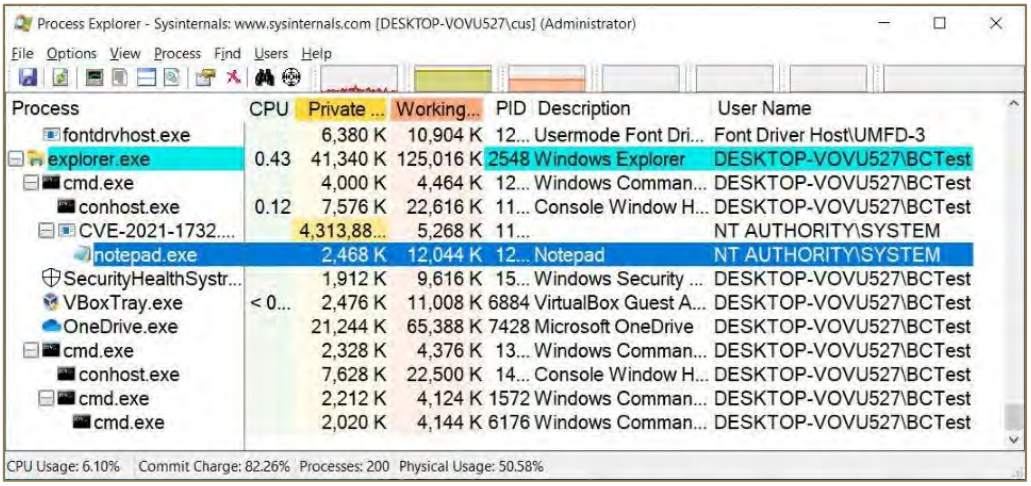
Windows vulnerability with new public exploits lets you become admin

Main Article

A security researcher has publicly disclosed an exploit for a Windows local privilege elevation vulnerability that allows anyone to gain admin privileges in Windows 10.

The vulnerability affects all supported versions of Windows 10 before the January 2022 Patch Tuesday updates.

Multiple exploits were publicly released for CVE-2022-21882 that allow anyone to gain SYSTEM privileges on vulnerable Windows 10 devices.



Many administrators chose to skip January 2022 updates due to the significant number of critical bugs introduced by the January 2022 updates, including reboots, L2TP VPN problems, inaccessible ReFS volumes, and Hyper-V issues the installation of these updates.

Action Points:

- If you have skipped or backed out of the Jan 2022 patches, look again at applying them and mitigating controls for these exploits.

All the best from all of us at **HEFESTIS** and look out for our next **Threatscape** update next week.

From: CISO Shared Service - UCSS <CISO-SHARE@JISCMAIL.AC.UK> **On Behalf Of** David Robertson
Sent: 04 February 2022 09:50
To: CISO-SHARE@JISCMAIL.AC.UK
Subject: David Robertson shared "Threatscape Newsletter" with you.

[CAUTION]This email originated from outside of the College - do not click links or attachments unless you recognise the sender and know the content is safe. If you have any concerns please contact ICT at ictservicedesk@glasgowkelvin.ac.uk.

Microsoft SharePoint

CISO Share

Threatscape Newsletter

Good morning and a very warm welcome to all of you from all of us at the Ciso Share Office.
Positive news again as no significant breaches are reported over January 2022 from the HE/FE sector in Scotland.
This week we cover the latest Microsoft security patching, with some vulnerabilities already identified. We not only look back at 2021 but also forward to trends in 2022.
Please check the CiSP site, as always, for the latest updates on current incidents and countermeasures to protect your institution.
Whilst you are here, why not drop into the CISO-Share user forum and discuss the latest topics and news.
Front and centre, Cyber Scotland week is getting closer, with the usual mix of interesting and informative sessions from across the public sector - including our good selves. Hope you can join in.
Here are a few of the articles which caught the attention of the CISO-Share team this week.
If you have any questions or comments please feel free to contact us.

Kind regards
David

David Robertson

M: 07852 330122
E: drobertson@hefestis.ac.uk

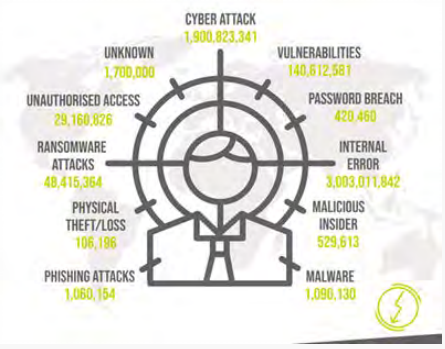
Steve McIntosh
M: 07904 908945
E: smcintosh@hefestis.ac.uk

Darren Clement
M: 07442 859979
E: dclement@hefestis.ac.uk

Cyber Scotland Week 28th February - 6th March 2022

This year's theme is "Learning for life online." Keeping everyone cyber aware and resilient. Main Website As always, a good idea to keep this event in the diary and attend the events which interest or have value for you. This year HEFESTIS will be h...

David Robertson
2/4/2022
2 views



List of data breaches and cyber attacks in January 2022 – 66 million records breached

If there was any belief that 2022 would see a sudden improvement in the cyber security landscape, our first list data breaches and cyber attacks of the year should end that hope. IT Governance discovered 95 security incidents in January, resulting i...

David Robertson
2/4/2022
5 views

UK organisations have experienced a 62% increase in cyber threats since 2020

Since the early days of the pandemic, experts warned that cyber criminals would thrive on new vulnerabilities and unfamiliar working conditions. However, few would have expected just how severe the threat would be. Main Article A Software Advice rep...

David Robertson

2/3/2022
2 views

Forensics as a Service (FaaS)

Digital forensics is a discipline that deals with the collection and analysis of systemic data and evidence after an incident or data breach has occurred in an organisation. The rapid adoption of Cloud Computing and remote working environment due t...

Steve McIntosh
2/4/2022
4 views

Phishing Links In LinkedIn

Phishers can take advantage of a marketing feature which lets them create a LinkedIn.com link that bounces your browser to other websites, such as phishing pages that mimic top online brands (but chiefly Linkedin's parent firm Microsoft). This is n...

Steve McIntosh
2/4/2022
2 views

Kaspersky stopped more than 30,000 attempts to use the Log4Shell exploit in January

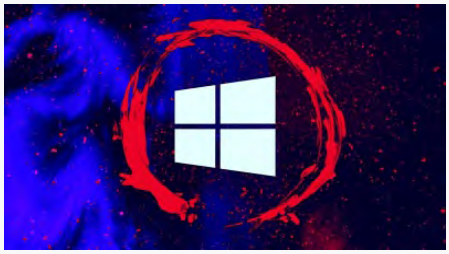
The critical remote code execution vulnerability in Apache's Log4j utility continues to be a popular tactic for cybercriminals. Consider this yet another plea to patch your systems. Main Article Cybersecurity company Kaspersky said it logged and blo...

David Robertson
2/3/2022
2 views

New Samba Bug Allows Remote Attackers to Execute Arbitrary Code as Root

Samba has issued software updates to address multiple security vulnerabilities that, if successfully exploited, could allow remote attackers to execute arbitrary code with the

highest privileges on affected installations. CVE-2021-44142 , rated 9.9 ...
Steve McIntosh
2/1/2022
4 views



Windows vulnerability with new public exploits lets you become admin

A security researcher has publicly disclosed an exploit for a Windows local privilege elevation vulnerability that allows anyone to gain admin privileges in Windows 10. The vulnerability affects all supported versions of Windows 10 before the Januar...
Steve McIntosh
2/1/2022
3 views

Go To Site

Get the SharePoint Mobile App

To unsubscribe from the CISO-SHARE list, click the following link:
https://www.jiscmail.ac.uk/cgi-bin/WA-JISC.exe?SUBED1=CISO-SHARE&A=1

HEFESTIS Weekly Newsletter

Good morning all and a warm welcome to this week's Threatscape where we highlight the new NCSC NMAP scripting collaboration, a targeted phishing attack against a member, our new member space in CiSP and the UK Governments cyber strategy.

Here are some of the week's Cyber Security articles which caught the attention of CISO-Share.

NCSC urge UK organisations to bolster their cyber security resilience

https://www.ncsc.gov.uk/news/uk-organisations-encouraged-to-take-action-around-ukraine-situation

UK organisations are being urged to bolster their cyber security resilience in response to the malicious cyber incidents in and around Ukraine.

While the NCSC is not aware of any current specific threats to UK organisations in relation to events in and around Ukraine, the guidance encourages organisations to follow actionable steps that reduce the risk of falling victim to an attack, including:

- patching systems;
- improving access controls and enabling multi-factor authentication;
- implementing an effective incident response plan;
- checking that backups and restore mechanisms are working;
- ensuring that online defences are working as expected, and;
- keeping up to date with the latest threat and mitigation information.

Action Point:

- Good recommendations for the best of times, more so now as there is concern around increased cyber activity attributed to Russia.

NCSC Scanning Made Easy

https://www.ncsc.gov.uk/blog-post/introducing-scanning-made-easy

Scanning Made Easy (SME) is a joint project between the i100 and the NCSC to build a collection of NMAP Scripting Engine scripts, designed to help system owners and administrators find systems with specific vulnerabilities.

SME scripts are written using the NMAP Scripting Engine (NSE). NMAP is an industry standard network mapping tool that has been in active development for over 20 years.

The first SME script we're releasing scans for are Exim message transfer agent (MTA) remote code execution vulnerabilities (CVE-2020-28017 through CVE-2020-28026, also known as 21Nails). Visit Github to download/view the script.

NMAP is one of my all time favourite security tools. This collaboration and output of scripts will help us all to find and resolve vulnerabilities faster.

Action Point:

- Evaluate the usefulness of NMAP and the scripts to increase identification and resolution speed.
- There are also development and submission guidelines so that any locally developed scripts can be shared.

  https://github.com/ukncsc/SME/blob/main/ncsc-scanning-made-easy-script-developer-guidelines.md

---

Member targeted phishing attack

https://share.cisp.org.uk/thread/14779

A member has reported receiving an extremely convincing targeted phishing attack. The phishing email redirected the recipient to a login page to harvest credentials. The malicious page had been constructed to look exactly like their real page with the links for help going to the institutions correct locations to further try and trick the victim.

Thankfully there were no victims and the malicious phishing email and site was reported so that action could be taken.

Action Point:

- Awareness training on how to identify a phishing email will reduce the number of victims.
- Having a simple, well known reporting procedure will allow swift action to take place on notification.

Implementing strong cybersecurity hygiene standards

https://www.securitymagazine.com/articles/96985-implementing-strong-cybersecurity-hygiene-standards

Cyber hygiene is about making sure you have the fundamental security controls operating and that they are consistently applied across your environment.

The core building blocks to cyber hygiene is knowing your estate and knowing your identities, this ultimately drives the controls you operate and provides a mechanism to understand how effective these controls are within your environment.

Effective approaches to adopting strong cyber hygiene processes include:

Secure Builds - Define secure build standards for the various platforms that your organization uses.

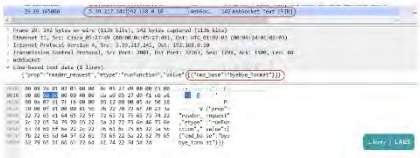
Secure Endpoints: Any and all corporate devices should be secured with strong endpoint controls, advanced malware protection, encryption, least privilege, and security event logging.

Authentication and Authorization: Standardize authentication and authorization, using strong authentication across the network and applications with MFA (Multi-Factor Authentication).

Identity and Entitlement: It is important to understand the identities within your environment, who they are associated with and the entitlements they have.

Action Point:

- Ensure that there is continuous monitoring of controls and established measures to understand the effectiveness of controls.
- Cyber hygiene practices need to be embedded throughout the organization to better protect your organization



Malware resets Android devices after performing fraudulent wire transfers

https://www.helpnetsecurity.com/2022/01/27/android-malware-reset/

BRATA was a RAT targeting Android users to capture and send user's screen output in real-time, log keystrokes, retrieve device information, turn off the screen to give the impression that it has been turned off, and more.

This banking focused attack chain usually starts with a fake SMS containing a link to a website and tries to convince the victim to download an anti-spam app, which gives the attacker control of the device and access to the 2FA code sent by the bank. In some cases, the link redirects the victim to a phishing page that looks like the bank's, and it is used to steal credentials and other relevant information.

Once they have the data they are factory resetting the device. This gives them time to empty out any accounts before the victim has time to recover and respond.

Action Point:

A particularly nasty attack, warn against the installation of applications out with the devices application stores, which are deemed to be whitelisted application for many frameworks.

Major Linux PolicyKit security vulnerability uncovered: Pwnkit

A serious memory corruption vulnerability in polkit (formerly PolicyKit) has finally been discovered after 12+ years. This program is found in essentially all modern Linux distributions.

Main Article

If it's not one thing, it's another. After one real Linux problem -- the heap overflow bug in the Linux kernel's fs/fs_context.c program -- is found and fixed, then a new security problem is discovered. This time security company Qualys has uncovered a truly dangerous memory corruption vulnerability in polkit's pkexec, CVE-2021-4034.

Polkit, formerly known as PolicyKit, is a systemd SUID-root program. It's installed by default in every major Linux distribution.

How dangerous is it? Very.

This vulnerability is easy to exploit. And, with it, any ordinary user can gain full root privileges on a vulnerable computer by exploiting this vulnerability in its default configuration. As Qualys wrote in its brief description of the problem: "This vulnerability is an attacker's dream come true."

Action Points:

Apply a patch as quickly as possible from your Linux distributor. If no patches are available for your operating system, you can remove the SUID-bit from pkexec as a temporary mitigation. For example, this root-powered shell command will stop attacks:

chmod 0755 /usr/bin/pkexec

Could you already have been attacked? It's possible. If there's been a sloppy attack on your system, see if there are traces in the logs. Typically this will be either "The value for the SHELL variable was not found in the /etc/shells file" or "The value for environment variable […] contains suspicious content."

But a sophisticated attacker can make a PwnKit assault without leaving any traces in the logs.

Apple Patches 'Actively Exploited' iOS Security Flaw

Apple late Wednesday pushed out an urgent iOS update with fixes for 11 documented security flaws and warned that one of the vulnerabilities "may have been actively exploited."

Main Article

In a barebones advisory, Apple acknowledged the zero-day took aim at a memory corruption issue in IOMobileFrameBuffer, an oft-targeted iOS kernel extension.

Learning Points:

As is customary the Cupertino, Calif. company did not share any details on the active exploitation or any indicators of compromise to help defenders hunt for signs of intrusion.

In addition to the documented zero-day, the iOS 15.3 patch addresses dangerous code execution flaws in ColorSync, kernel, and the WebKit rendering engine.

The update also covers privilege escalation, data leakage, and denial-of-service flaws in multiple iOS components.

Separately, Apple pushed out a security update for macOS Catalina to fix multiple security issues and a Safari browser patch covering multiple WebKit security defects.

Emotet Now Using Unconventional IP Address Formats to Evade Detection

https://thehackernews.com/2022/01/emotet-now-using-unconventional-ip.html

Emotet-related attacks aim to trick users into enabling document macros and automate malware execution.

In these spotted instances, once enabled, the macro invokes a URL:

"h^tt^p^:/^/0xc12a24f5/cc.html" or
"h^tt^p^:/^/0056.0151.0121.0114/c.html"

This involves the use of hexadecimal and octal representations of the IP address

Evasion techniques like these could be considered evidence of attackers continuing to innovate to thwart pattern-based detection solutions.

Action Point:

Check to see if your pattern matching solutions can detect obfuscated IP addresses, if they do not investigate how this can be achieved.

NEW - HEFESTIS CISO Share Members Forum on CiSP

We are very pleased to announce that CiSP have given us our very own, secure HEFESTIS members area.

Link to HEFESTIS CISO Share forum

The link is also available from this Sharepoint site launched from the "Forum" tile on our main landing page.

You must be a member of CiSP to access this forum which you can also find on the main web-site by searching for HEFESTIS CISO Share from the "places" area.

Because the forum is restricted to members only, you will have to ask to join.

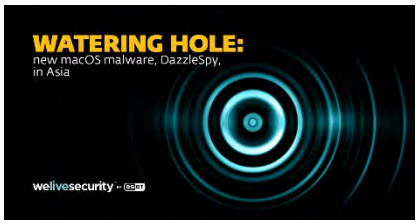
The HEFESTIS CISO Share Forum is a secure area where members and the CISO Share team can post articles of interest, alerts, chat and incident information - in fact anything related to cyber security which will stay confidential to the HEFESTIS community at all times.

It may be considered for use as an emergency channel should there be a significant communications outage - pre-registration for key incident responders and teams will facilitate immediate access to the forum should an incident occur.

This is your area which we will support and develop in line with your feedback and suggestions. We look forward to some interesting interactions.

Action Point:

Why not join and start a conversation today?



New macOS Malware 'DazzleSpy' Used in Hong Kong Attacks

A recent campaign targeting individuals in Hong Kong has leveraged at least two pieces of malware designed to target macOS systems.

Main Article

Technical Info

In November 2021, Google shared details about an attack where macOS malware was delivered to users in Hong Kong via compromised pro-democracy websites that served as watering holes.

According to Google, the attack, discovered in late August, was likely conducted by a well-resourced state-sponsored threat group.

Action Point: The attackers leveraged both iOS and macOS exploits. The macOS exploit involved a WebKit remote code execution vulnerability patched by Apple in January 2021 (CVE-2021-1789) and a privilege escalation flaw that Apple patched in September, roughly one month after the attack was spotted by Google's security researchers.

UK Government Cyber Security Strategy for 2022-2030

https://www.gov.uk/government/publications/government-cyber-security-strategy-2022-to-2030

The UK Government has released a Cyber Security Strategy for 2022-2030.

The Cyber Security Strategy explains how the government will ensure that all public sector organisations will be resilient to cyber threats.

The strategy's vision is to ensure that core government functions are resilient to cyber attack, strengthening the UK as a sovereign nation and cementing its authority as a democratic and responsible cyber power.

The contents are very similar to the Scottish Governments Cyber Resilience Framework, and devolved Governments have responsibility over this area with an agreement to collaborate.

They have added staff recruitment, retention and development which is nice to see as that is a major issue at the moment.

Action Point:
Have a look at the strategy to see how it aligns, or can further benefit our own through adoption of any missing, relevant areas.

Data of 7 Million OpenSubtitles Users Leaked After Hack Despite Site Paying Ransom

OpenSubtitles Hack Shows Why Paying Ransom Offers No Guarantees

Main Article

Popular subtitles website OpenSubtitles on Tuesday admitted that its systems had been hacked after the details of nearly seven million user accounts were leaked, despite the site allegedly paying a ransom to avoid this situation.

Law enforcement and cybersecurity professionals have often advised against paying a ransom to cybercriminals as it encourages them to continue their malicious activities, and there is no guarantee that the attacker will hold up their end of the bargain. The OpenSubtitles hack is a perfect example of this.

According to a forum post from OpenSubtitles' administrator, the opensubtitles.org website was hacked by someone in August 2021. The attacker had exploited a series of vulnerabilities to obtain user data and then asked for an undisclosed amount of bitcoin in exchange for not making the hack public and deleting the data.

Action Point:

Never trust a ransomware extortion request - consider using our ransomware evaluation tools and guidance to support decision making on whether or not to pay any ransomware demand

The Have I Been Pwned breach notification service has identified more than 6.7 million user records, including username, email, IP address, country, and unsalted MD5 password hash.

Ransomware policy considerations

Cyber Incident Risk Impact and Cost Benfit Assessment 5x5

Ransomware Cost Benefit Matrix Guidance 5x5

All the best from all of us at **HEFESTIS** and look out for our next **Threatscape** update next week.

HEFESTIS

2021

Microsoft Teams Review

DPO SHARE SERVICE

15/12/21

HEFESTIS | dpo@hefestis.ac.uk

1. Introduction

Microsoft Office 365 (O365) is now widely used across the HE/FE sector. For many institutions, roll-out began pre-covid, but there is no doubt that the pandemic has expedited the process and created the business case for 'blended learning' resulting in others following suit.

With the use of Microsoft Teams – a relatively new platform - increasing, new functionality being introduced and different site set-up approaches, we are seeing some issues arising in the data protection space. This briefing note has been produced for our members to raise awareness of some of these issues the DPOs have identified so that they can consider these relative to their organisation to support compliance. Some of the issues identified will not be limited to the use of Microsoft Teams.

2. Keep Teams private

ISSUE: Microsoft Team sites are set-up as 'public' instead of 'private'. This has resulted in students and/or staff running searches on college infrastructure, with 'public' Teams sites appearing in the search results, which (unhelpfully) provides some information from the site, resulting in a data security breach. Ensure adequate restrictions are in place to prevent unauthorized access or sharing of Microsoft Teams sites and content, and lock-down apps so that only those approved by your organisation can be used.

CAUSE: Human error and inadequate restrictions applied. There is no option currently available to default sites to 'private' setting. Most of these breaches have occurred at colleges and organisations that do not manage their Teams sites centrally (i.e. IT Team). This also applied to restricting access and sharing of sites and app use. This increases the risk of breaches, as rather than a limited number of individuals following a procedure regularly, lots (100s) of staff will do this infrequently, as required.

SOLUTION: Ensure all Teams sites are set as 'private' (preferably by default if this becomes possible). Manage Teams sites centrally e.g. via IT. Ensure regular audits are conducted to identify and remove inactive and redundant Teams sites.

3. Be mindful of data retention

ISSUE: Documents and data held in Microsoft Teams may prove problematic in relation to Subject Access Requests (SARs) if data can be retained indefinitely (think email retention and SARs). This has the potential to generate lengthy, resource intensive SARs responses. Chat logs can cause problems, not just due to indefinite retention of them but also the informal nature of chats. Personal data contained in chats can be disclosable as part of a SAR.

CAUSE: No retention period set for Teams chat.

SOLUTION: Consider implementing retention policies for Microsoft Teams chat logs e.g., of three months as a measure to limit the scope of any search to a reasonable level. Staff should be reminded that appropriate language and phraseology should be used, bearing in mind that what someone 'chats' about might be disclosable to the data subject.

4. Be mindful of data minimisation

ISSUE: Recording of Microsoft Teams information, including meetings, may prove problematic in SARs (how would you redact a Teams meeting as part of a SAR?). This has the potential to generate lengthy, resource intensive SARs responses.

CAUSE: Processing of personal data unnecessarily. Just because technology allows for it, doesn't mean you should.

SOLUTION: Consider if you need to record Microsoft Teams meetings. Limit this to an absolute minimum, with tight retention periods so the data is used for the purpose for which it was collected and then deleted.

5. Be aware of automatically generated Microsoft Teams email accounts

ISSUE: When a Teams site is created an associated email account is created by default. These accounts are included in an organisation's Global Address Book and individuals may send emails to them assuming they are managed accounts. Teams site members may be unaware of these email accounts, and they may not be monitored for incoming mail. Additionally, all Teams site members can access the emails, and this may result in inappropriate access to personal data, particularly when there are members of a Team site who are external to the college (from another organisation).

CAUSE: When a Teams or SharePoint site is created an email address for that site is automatically created. The email address is available in the Global Address Book for anyone to contact.

SOLUTION: Advise that these email addresses should never be used to send a message containing personal data, as it will become public by default, on the relevant Teams timeline.

6. Be mindful of disclosing names/email addresses using Microsoft Teams meeting requests

ISSUE: Microsoft Teams exposes guest e-mail addresses by default, posing a privacy risk because of a data breach, where names are contained in email addresses, potentially exposing guests to unwanted communication from others.

CAUSE: When an individual is invited to join a meeting their email address is visible to all members of the group. This can be a problem if the person is external to the organisation and/or using a personal email address. There is no fix to this problem yet. A short-term solution could be to advise individuals to create a separate email address for communication with this group if they do not want to share their current personal email address. Alternatively, the invite can be sent to an individual (i.e. the meeting organiser) and forwarded to the proposed attendees.

Teams or SharePoint site is created an email address for that site is automatically created. The email address is available in the Global Address Book for anyone to contact.

SOLUTION: HEFESTIS has written to Microsoft on behalf of members to raise this issue stating the administrator at least should be able to control this, easily and at a local level.

7. Conclusion

HEFESTIS Members should:

- be aware of these known issues and mitigate the risks,
- ensure staff are aware of these known issues and know how to mitigate the risks through Microsoft Teams guidance and training,
- ensure appropriate policies, procedures and administration are in place to support staff in their use of Microsoft Teams.

Glasgow Kelvin College

Risk Management Committee

Minute

Meeting held on Tuesday 25 January 2022 at 2pm online using Microsoft Teams

Item	Action Agreed	Member
1	**Sederunt**	
	L Clark welcomed members to the meeting that commenced at 2pm and was attended by the following members: L Clark, Director of Corporate Services (Chair); J Evans, Vice Principal Operations (left 3pm); D Shiels, Director of Human Resources; A Daly, Finance and Student Funding Manager; E Campbell, Head of Funding (representing A McGhee); E Mitchell, Senior Human Resources Business Partner; G McGuire, Senior Curriculum Manager HCCLD (representing T Leavy); G Lawson, Health and Safety Manager; I Gordon, Head of Facilities and Environmental Sustainability; J Quinn, Director of Digital Services; J Clarke, Senior Curriculum Manager BCI (representing A Allan); J Gallagher, Quality Enhancement Development Manager; M Smillie, Head of Student Information Service; M McKerlie, Head of Services to Support Learners; M Thomson, Team Leader Administration; R MacKenzie, Senior Administration Officer; and J Carroll (recording purposes only).	
2	**Apologies**	
	D Smeall, Principal; A Carr, Head of Finance; L Lang, Communication and Planning Manager; and P Brown, Director of Planning, Performance and Curriculum.	
3	**New Terms of Reference**	
	Members noted the content of the new Terms of Reference for information purposes.	
4	**Draft Minute of Previous Meeting held on 2 November 2021**	
	The minute was accepted as a true and accurate record of the business conducted at the previous meeting.	

Item	Action Agreed	Member
5	**Matters Arising from the Minutes of the Previous Meeting**	
	Item 3: Terms of Reference	
	D Shiels confirmed that the Equality Access and Inclusion post would be filled imminently. This person would be invited to join the Risk Management Committee.	
	Item 5: GDPR/Cyber Security	
	L Clark and J Quinn would liaise regarding matters identified at the Cyber Security Audit that included Phishing training, logging/intrusion detection and mandatory cyber security training.	**LC/JQ**
	Item 5: Risk Appetite and Risk Register Review	
	G Lawson raised members awareness that the college required Fire Wardens with training organised for the next staff development day for appropriate staff.	**ALL**
	D Shiels reported that the College currently records and reports separately absence rates associated with mental health as part of absence management monitoring processes.	
	Item 8b: Asset Management/News Articles from City of Glasgow	
	L Clark reported that the Fixed Asset Register had been reviewed and was currently being amended.	
	Item 8e: Data Retention Schedule	
	L Clark and J Quinn would meet to discuss recommendations for threads within Microsoft Teams, which should be restricted to a maximum 3-month duration to the impact from Subject Access Requests (SARs).	**LC/JQ**
	Item 9a: Domestic/International Travel Advice	
	L Clark reported that clarity was required regarding automated travel process with arrangements being made through liaison with the Procurement Officer.	**LC**
	Item 15: Risk Management	
	G Lawson reported that First Aid schedules were now full and that there was a requirement for additional First Aiders at West Campus.	
	G Lawson reported that additional Fire Wardens were required at Springburn Campus.	**GL**

Item	Action Agreed	Member
6	**Health and Safety**	
a)	**Health and Safety Minute 17 September**	
	G Lawson summarised the content of the Minutes that included a new traffic light system for WorkRite Health and Safety training which was more user friendly.	
	It was decided that Legal Current Issues Review (LCIR) would be considered by this Committee for information purposes at all future meetings.	**GL**
	Members noted the content of the Health and Safety Minute for information purposes.	
b)	**Draft Health and Safety Minutes: 10 November 2021**	
	Members noted the content of the Health and Safety Minutes for information purposes.	
7	**Finance**	
	J Evans reported that Management Accounts Quarterly Forecasts were now available and that the Finance and Student Funding Manager and the Bursary Team Leader were now responsible for all support funding.	
	She highlighted that UNISON feedback was expected shortly.	
8	**GDPR/Cyber Security**	
	R MacKenzie reported that the Data Protection Audit, to be conducted by Henderson Loggie, would take place from 21 February 2022 to 24 February 2022.	**RMcK**
	R MacKenzie reported that the GDPR internal audit of the Finance Office, to be conducted by the College Data Protection Officer, would take place shortly.	**RMcK/ AD**
	J Quinn reported that Cyber Essential Plus Certification would be scheduled annually.	
	He advised members that Log4J vulnerability was currently a low risk to the college with appropriate counter arrangements already made, but that it remained a threat within the sector. He requested staff to stay vigilant and verify at all times.	
	He reported that he would review the ICT Penetration Report.	**JQ**

Item	Action Agreed	Member
9	**Insurance**	
	L Clark would ensure that Insurance was value for money through liaison with the Procurement Officer.	**LC**
10	**Estates**	
a)	**Capital and Sustainability Update**	
	I Gordon requested members to note the content of the Estates Capital Report for GCRB for information purposes that was on track to achieve spending requirements by 31 March 2022 regarding improvements in the college estate.	
	There followed a considerable discussion regarding a dislodged panel at the Springburn Campus that had occurred; it was agreed that L Clark and J Quinn would discuss this further.	**LC/ JQ**
	Members noted the content of the Capital and Sustainability Update for information purposes.	
b)	**UK Government: Protect Duty Consultation - Government Response Document**	
	M Thomson spoke to the content of the Protect Duty Response Document reporting that Risk Assessment staff training through eLearning would be take place before the end of the year.	**MT**
	She reported that the Incident Management Team would shortly take part in a training exercise.	
	Members noted the content of the UK Government Response Document for information purposes.	
c)	**UK Home Office and The Rt Hon Priti Patel MP: Government Publishes Protect Duty Consultation Findings News Story**	
	Members noted the content of the UK Government News Story for information purposes.	
11	**Human Resources**	
	D Shiels encouraged members to raise staff awareness of the positives on being on campus to steer wellbeing matters.	**ALL**
	She reported that work was ongoing on the Recruitment system and Cintra regarding Data Protection through liaison with ICT.	

Item	Action Agreed	Member
12	**Risk Management**	
	a) Risk Management Framework	
	J Evans summarised Risk Management within the College reporting that Team Risk Registers would be aligned twice per year, which would be scheduled next week.	**JE**
	Members noted the content of the Risk Management Framework for information purposes.	
	b) Risk Registers Channel	
	J Evans reported that Team Risk Registers were live on Microsoft Teams and should be updated accordingly as appropriate by Team Members.	**TM**
	M McKerlie, M Smillie and A Daly - access to Risk Registers would be checked to ensure these arrangements had been established.	**JC**
	Members noted the content of the document containing the link to the Risk Registers Channel for information purposes.	
	c) Strategic Risk Register	
	J Evans informed members that the Strategic Risk Register was read only for Managers and outlined that the following would take place at the next meeting:	
	• Risks would be scrutinised individually, especially regarding mitigation.	**ALL**
	• Departmental Risk Summary would be provided by individual Team Members	**ALL**
	J Quinn spoke about pulling information into Dashboard and embedding the operational college cycle which would be discussed with J Evans on Thursday 28 January 2022.	**JE/ JQ**
	Members noted the content of the Strategic Risk Register for information purposes.	

Item	Action Agreed	Member
13	**Items for Information**	
	a) CCTV Cameras	
	I Gordon reported that CCTV cameras were being used on the fourth floor at Springburn Campus as a deterrent to incidences of vandalism. Students had been reported throwing objects from the fourth floor down into the Library area on the ground floor with a high risk that serious injury could occur.	
	Members agreed that the plant arrangement in the Springburn Foyer would be removed to stop learners throwing decorative stones.	**IG**
	b) East End Garden: Vandalism	
	I Gordon spoke about actions to counteract vandalism with a temporary tower installed at considerable cost at East End.	
	Members noted the content of the photographs of vandalism at East End Campus provided for information purposes.	
	c) HEFESTIS Newsletters from 5 November 2021 to 14 January 2022	
	R MacKenzie raised salient points from the HEFESTIS Newsletter including LG4J Vulnerability, Phishing, Cybercrime, protocols for homeworking and scams using Sky digital services for extortion by cyber-criminals.	
	G McGuire reported that he would raise these points with the Director of Community Engagement and Curriculum to endeavour to raise awareness.	**GMcG**
	Members noted the content of HEFESTIS Newsletters for information purposes.	
	d) Audit Scotland Publication: Technical Bulletin 2021/23	
	Members noted the content of the Audit Scotland Bulletin for information purposes.	
	e) Daily Record: Scotland 'racing headlong into a teen gang crisis' with kids 'as young as 11 tooling with knives' News Article	
	Members noted the content of the Newsletter for information purposes.	

Item	Action Agreed	Member
14	**Equality Management - Equality issues to be considered as a consequence of the consideration of the above**	
	Members agreed that the following new Equality Management issues had arisen as a consequence of the above agenda. • high absence rates regarding poor mental health would be considered in the review of the Attendance Management and Support Policy and Procedure, which was due for renewal.	
15	**Risk Management - Risk issues to be considered as a consequence of the consideration of the above**	
	Members agreed that the following Risk Management issues had arisen as a consequence of the above agenda.	
	• Fire Wardens required at Springburn Campus;	
	• Cyber Security Audit: Follow up action; and	
	• Imminent GDPR Audit.	
16	**Data Protection – Data Protection issues to be considered as a consequence of the consideration of the above**	
	Members agreed that the following Data Protection issues had arisen as a consequence of the above agenda.	
	• SFC Audit; and	
	• Data Protection Audit.	
17	**Closure**	
	L Clark thanked members for their contributions to the meeting. The meeting closed at 3:10pm.	
18	**Date of Next meeting**	
	Tuesday 19 April 2021 at 2pm online using Microsoft Teams.	

LC/JC
Glasgow Kelvin College
1 February 2022