APPENDIX 2 – NOT IN THE PUBLIC DOMAIN

Item 13
For Noting

Glasgow Kelvin College

Audit and Risk Committee Meeting of 22 February 2022

ICT Update

Report by Director of Digital Services

1. Introduction

The purpose of this report is to update Board members on Cyber Resilience matters within the College. This will include an update on the threat outlook to the Further Education sector, activities that have been carried out to improve Cyber Resilience within the College and future initiatives which will further protect the organisation.

2. Threat Outlook

Ransomware continues to be the leading cause of security incidents for organisations, with phishing being the dominant vector for initiating the cyber-attack. High profile attacks continue to be reported in the news and will often result in a significant financial impact through payment of the ransom or the cost of rebuilding the IT infrastructure. The full financial cost to SEPA after their December 2020 cyber-attack, is still being counted by their management team. Gloucester City Council have set aside £380,000 to restore their IT systems after an attack in December 2021. The financial and reputational risk to a cyber-attack can be significant.

The risk to data loss is also of concern, with cyber criminals again targeting organisations. However, data breaches were more likely to emanate from human error in 2021, highlighting the need to educate users of systems on the risks of mishandling data and how this can be avoided.

The College recognises the threat is growing and the impact to operations can be significant. While an attack likelihood is considered probable, several mitigations have been implemented to reduce the impact and risk of a cyber-attack, including a staff digital skills information portal, multiple factor authentication to secure user accounts, remote software update of College laptops, system backups, use of cloud technologies, incident management, and a range of hardware security controls for IT infrastructure.

3. Operational Updates

3.1 Cyber Essentials Plus Certification

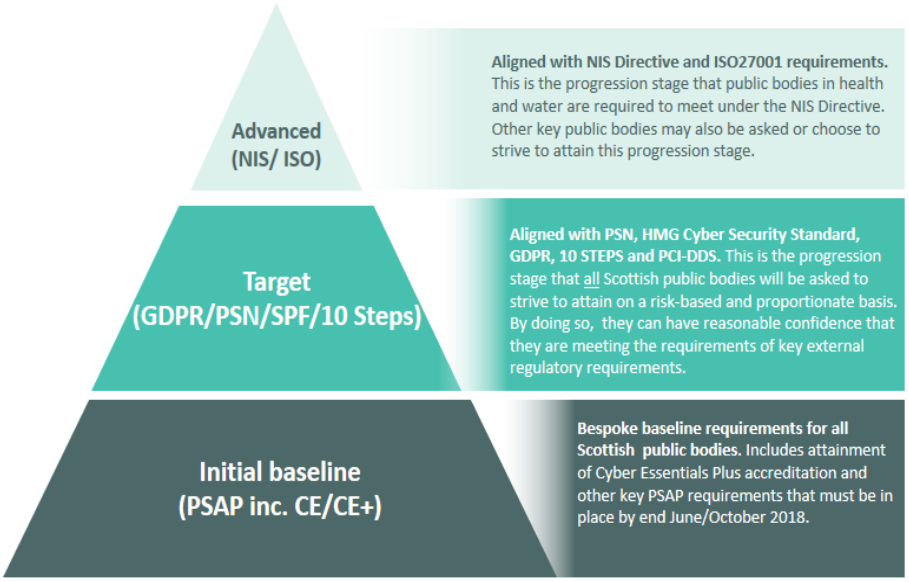
The ICT team delivered a successful recertification of the Cyber Essentials Plus scheme in December 2021 Appendix 1 - Cyber Essentials Plus Certificate . The scheme is a requirement for public sector bodies and forms part of our 'initial baseline' assessment as set out in the Scottish Government's Cyber Resilience Framework. The annual assessment continues to challenge and test our cyber

resilience measures, ensuring that we maintain the high level of compliance expected of us.

The Cyber Essentials Plus assessment comprises of the following five practical tests, all of which must be passed and evidenced before a Cyber Essentials Plus certificate may be awarded.

- External vulnerability scan
- Internal vulnerability scan
- Verify malware protection
- Email security check
- Web browser security check

Furthermore, the College continues to develop its cyber resilience capability and is progressing towards the 'target' standard as defined in the Scottish Government's Cyber Resilience Framework.



More information can be found on the Scottish Governments website - https://www.gov.scot/publications/cyber-resilience-framework/.

3.2 Network Penetration Testing

As part of our commitment to continuous review of the College ICT cyber resilience, we commissioned Barrier Networks to conduct a security assessment of the internal infrastructure. The assessment was from the perspective of a trusted college system user with the aim of identifying weaknesses and vulnerabilities within our digital environment, and to provide long term remediation recommendations to strengthen our overall cyber security.

The assessment was conducted remotely between 28th September 2021 and 1st October 2021. A total of 13 recommendations were identified – two rated critical, four rated high, and seven rated medium. Remedial action has now been completed by the ICT team, which contributed to our successful Cyber Essentials Plus certification.

3.3 Zero Trust Network

Throughout January and February 2022, the ICT team have been working alongside Khipu Networks to install a Zero Trust Network. This approach to security is the next evolution for the College IT systems and supports our current hybrid method of working. The aim is to implement technologies that provide an adaptive trust model, where access to resources and data is only granted where necessary through continuous authentication and trust is never implicit.

The deployment of a Zero Trust Network is a design architecture to enable the College to securely deliver remote digital learning, facilitate hybrid working for staff, securely deploy cloud infrastructure, encourage the use of personal devices for students, and mitigate sophisticated cyber-attacks using multiple exploits methods.

Further information can be found here: What Is Zero-Trust Networking? - Cisco.

4. Future Plans

4.1 Cyber Risk Technical Assessment

The College has a range of cyber-security controls in place, which need to be tested regularly to ensure they provide the level of protection required for new and emerging threats. The ICT team has engaged Barrier Networks to provide an external technical review of the deployed security controls in the form of a Cyber Risk Technical Assessment (CRTA). A CRTA provides an increased level of assurance that technical cyber risk is being reduced to an acceptable level. It is conducted by an experienced security architect who reviews the security architecture and deployed technical controls to identify where gaps in the security posture may be present.

Barrier Networks will work with the College with the objective of identifying cyber risk and reviewing technical controls to ensure they have been configured correctly and are working as expected. Technical components such as firewalls, email gateways and endpoint security will be assessed to determine if they are implementing security policy appropriately. The assessment is expected to take place in March 2022.

The controls reviewed will be documented within the final report in May 2022, and recommendations will be provided to advise where these can be improved. These recommendations will help the ICT team to structure our security strategy based on the risks identified and to improve the effectiveness of existing security investments.

4.2 Cloud ICT Infrastructure

The ICT team are investigating the potential for hosting and migrating ICT hardware and infrastructure, traditional hosted on-premises, to the Cloud. Infrastructure under consideration are the College servers, backup systems and the telephone system. The team are engaging with third-party suppliers, colleagues in the sector and undertaking their own research to determine the feasibility and suitability for any proposed solution.

Hosting infrastructure in the Cloud brings many benefits, particularly given the agility it brings in facilitating business continuity through hybrid working and the continuation in delivery of education. It also delivers on the ambitions set out in our Digital Transformation Strategy, however in doing so it introduces a new layer of complexity and risk which will require expert planning and upskilling in the workforce.

5. Resources Implications

There are no immediate resource implications assigned to this report. Future investment may be required to ensure the College is able to deliver on strategic ambitions and to reduce the risk of new and emerging cyber-threats, however sustainable financial choices will always be considered in any investment requirements.

6. Equalities

No adverse impacts on individuals with protected characteristics have been identified as a consequence of this report.

7. Risk and Assurance

By undertaking the aforementioned actions, the Committee can be assured that the College are taking their responsibilities in relation to cyber crime and awareness raising very seriously, thus mitigating the risk as far as possible. The College meets the high standards set by the Scottish Government in terms of cyber resilience.

8. Data Protection

There are no data protection concerns with the contents of this report which has been marked as Not in the Public Domain. It is accepted that a cyber attack brings real concerns of data loss, subsequent fines and reputational damage. The actions as outlined in this report will reduce the risk of data loss.

9. Recommendations

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

10. Further Information

Members can obtain further information on the contents of this report from Jason Quinn, Director of Digital Services – jquinn@glasgowkelvin.ac.uk.

Glasgow Kelvin College
Jason Quinn
February 2022

Appendix

CYBER ESSENTIALS PLUS

CERTIFICATE OF ASSURANCE

Glasgow Kelvin College

COMPLIES WITH THE REQUIREMENTS OF THE CYBER ESSENTIALS PLUS SCHEME

NAME OF ASSESSOR :

CERTIFICATE NUMBER :

PROFILE VERSION : April 2020

SCOPE : Whole organisation

DATE OF CERTIFICATION : 2021-12-30

RECERTIFICATION DUE : 2022-12-30

CERTIFICATION MARK

CYBER ESSENTIALS CERTIFIED PLUS

CERTIFICATION BODY

BARRIER NETWORKS

CYBER ESSENTIALS PARTNER

IASME CONSORTIUM

The Certificate certifies that the organisation was assessed as meeting the Cyber Essentials Plus implementation profile and thus that, at the time of testing, the organisation's ICT defences were assessed as satisfactory against commodity based cyber attack. However, this Certificate does not in any way guarantee that the organisation's defences will remain satisfactory against a cyber attack.