GCRB Glasgow Colleges' Regional Board

Audit Committee Meeting

Date of Meeting	Tuesday 29 May 2018
Paper Title	Cyber Security
Agenda Item	15
Paper Number	AC4-K
Responsible Officer	Jim Godfrey, Finance & Resources Director
Status	Disclosable
Action	For Noting

1. Report Purpose

1.1. This paper provides a summary of the actions in response to the risks to Cyber Security.

2. Recommendations

2.1. The Committee is asked to **note** the:

- Scottish Government's Cyber Resilience Strategy for Scotland, the key actions arising therein and progress by GCRB.
- Assessment of Cyber risk to GCRB and the proposed actions.
- Draft ICT Strategy (for the College Sector) and the issues relating to Cyber Security.
- (Summary) Cyber Security Strategy of City of Glasgow College, upon which GCRB places reliance for its core IT systems.

3. Cyber Resilience Strategy

3.1. Published in November 2017, by the Scottish Government, the Cyber Resilience Strategy for Scotland details the actions to be taken to protect public bodies from cybercrime. A copy of the full report is available via the following link: http://www.gov.scot/Resource/0052/00527399.pdf

3.2. By undertaking the actions set out in this plan, public bodies are adopting a consistent approach and providing assurance to service users. A list of the actions is provided as an Annex to this report.

3.3. This report aims to show how GCRB will develop its resilience to cybercrime. The following are the key actions identified in the Cyber Resilience Strategy for Scotland together with a comment re progress:

Actions	Progress
Develop a common approach to cyber resilience in Scottish public bodies.	Utilisation of the Cyber Resilience Strategy by GCRB will ensure that its approach is aligned with other public bodies and the Glasgow colleges.
Have in place minimum cyber risk governance arrangements by June 2018.	The purpose of this report is to guide GCRB's response to cyber risk,
Ensure the public bodies that manage their own networks become active member of the NCSC's Cybersecurity Information Sharing Partnership (CiSP).	Not directly applicable to GCRB. Enquiries to be made of the Glasgow colleges to ascertain their membership status.
Ensure the public bodies have in place appropriate independent assurance of critical cyber security controls by October 2018.	Enquiries to be made of the Glasgow colleges to determine their plans to put in place independent assurance of controls.
Have in place appropriate cyber resilience training and awareness raising by June 2018.	Basic training undertaken by Finance & Resources Director. Cyber resilience discussed at Executive Meetings and also at Joint Audit Meeting. Further training planned.
Have in place appropriate cyber incident response plans by June 2018.	A short incident response plan to be developed by Finance & Resources Director.
Supply chain cyber security arrangements to be review for supply chain and grant recipients.	Finance & Resources Director to request, and review, cyber security plans of the Glasgow colleges.
Scottish Government will put in place innovative Dynamic Purchasing System for Digital Services.	Finance & Resources Director to research this in further detail to understand the opportunities for GCRB.
Scottish Government to promote leadership and knowledge sharing.	Limited information is available currently on this development and the Finance & Resources Director will continue to monitor.
Scottish Government will put in place a monitoring and evaluation framework to assess progress.	Finance & Resources Director to monitor developments and implement as appropriate.

3.4. The Committee is invited to note the response of GCRB to the actions identified in the Scottish Government's Cyber Resilience Strategy.

4. Assessment of risk to GCRB

4.1. At the outset it is important to examine the risks faced by GCRB, in order to inform the response.

4.2. The first risk that might be considered is the impact of cybercrime on the systems and equipment used by GCRB. As GCRB uses the computers, and network, of City of Glasgow College it is likely that the risks will be faced by the college as a whole. As such, GCRB can place reliance upon the security systems already in place within the college. Therefore the direct risk to GCRB is relatively low and we benefit from the considerable investment in security be the college.

4.3. The second risk is the impact of cybercrime on the data held by GCRB. In a similar manner to the comment above, the network security provided by the college helps to protect the security of stored data. The other risk occurs when data is lost, or stolen, when it is being sent to/from GCRB. Of the two areas identified, it is considered that the greatest risk to data is when it is in transit, or stored within emails, presents the higher risk.

4.4. In adopting a risk based approach, GCRB will focus resources on actions that can have the biggest impact. The following actions are planned:

Action	Owner	Timescale
Develop a protocol for the transfer of data in/out of GCRB.	Finance & Resources Director	31 July 2018
Review and delete historic documents that are no longer required.	GCRB Executive	31 August 2018
Consider the implementation of a secure file transfer system.	Board Secretary	Report to be presented to the Board meeting on 18 June 2018.

4.5. The Committee is invited to note that GCRB will undertake specific actions in response to an assessment of Cyber risk.

5. Draft Sector ICT Strategy

5.1. A draft ICT Strategy has been prepared for the college sector. This strategy has been developed by the Further and Higher Education ICT Oversight Board, which oversees national level actions and collaboration on ICT, working with Jisc[1], UCSS-ISSC[2] and others.

5.2. The full strategy is not yet in the public domain, however, the draft document outlines some of the aims in respect of cyber security:

- "To meet Scottish and UK Government requirements to have demonstrable cyber security controls in place, we will encourage universities and colleges to align their work on cyber resilience with the Public Sector Action Plan on Cyber Resilience, and the planned Public Sector Cyber Resilience Framework (when finalised). As part of this work, we will examine options for certification/accreditation against agreed standards such as Cyber Essentials, Cyber Essentials Plus or ISO 27001. The adoption of the controls within these schemes will enhance core cyber resilience within individual institutions and will also provide assurance to third party partners and internal users."

- "We will continue to work collaboratively across the sector, and beyond, to share threat information, utilising membership of the National Cyber Security Centre, CiSP3 scheme, whilst leveraging the HEIDS[4] IS network of sector contacts to share experiences and good practice guidance. Additionally, to drive further benefit across the sector, we will share training and awareness resources and exploit digital training solutions where possible. We will also encourage joint initiatives to allow sharing of costs and will foster contacts with other sectors to gather broader experiences that might benefit individual institutions or the broader sector."

5.3. In developing its approach to cyber security, GCRB will take cognisance of the national ICT strategy.

[1] Jisc (formerly Joint Information Systems Committee) is the UK higher, further education and skills sectors' not-for-profit organisation for digital services and solutions.

[2] Universities and Colleges Shared Services – Information Security Shared Service

[3] Cyber Security Information Sharing Partnership – a joint industry and government initiative to exchange cyber threat information.

[4] Higher Education Information Directors Scotland – a group of IT specialists in the Higher Education Sector.

6. City of Glasgow College – Cyber Security Strategy

6.1. City of Glasgow College kindly provides IT systems and services to GCRB. As such, GCRB is dependent upon the security arrangements that the college implements regarding its IT systems.

6.2. City of Glasgow College are working towards Cyber Essentials Plus in accordance with the Scottish Government Cyber Resilience Action Plan with an anticipated date for completion of October 2018. In the meantime, the college continues to follow an approach to IT security which includes the following measures:

- Installation/Active maintenance of Anti-Virus products on all desktops.
- User account creation/management procedures to ensure only authorised access.
- Anti-Spam filtering to prevent viruses via email.
- Web filtering and Malware detection.
- Key IT staff subscribed and participating in various security groups.
- Patching of key vulnerabilities in systems.
- Perimeter firewalls with regularly reviewed filter rules.
- Segmentation of 'bring your own devices' to ensure that 3rd party devices are isolated.
- Regular internal and external scanning to determine system vulnerabilities.
- Developed Acceptable Use and Social Media policies.

6.3. GCRB places reliance upon the security arrangements of the college and can therefore have confidence the systems it uses.

7. Legal Implications

7.1. There are no legal implications arising from this report.

8. Resource Implications

8.1. There are no direct financial implications as a result of this report.

9. Strategic Plan Implications

9.1. Through the conditions of grant associated with the Regional Outcome Agreement, GCRB is required to conduct its affairs in accordance with the expected standards of good governance, which include establishing appropriate arrangements in relation to risk.

A Cyber Resilience Strategy for Scotland
Public Sector Action Plan 2017-18

A. Developing a common approach to cyber resilience in Scottish public bodies

■ **Key Action 1:** The Scottish Government will work with the NCRLB, the National Cyber Security Centre (NCSC), the Scottish Public Sector Cyber Catalysts and other key partners to develop a Cyber Resilience Framework for Scottish public bodies by end June 2018. This framework, with associated guidelines and requirements, will help promote a common, effective, risk-based approach to cyber resilience across Scottish public bodies. A high-level concept framework can be found at Annex B.

B. Initial baseline cyber resilience requirements for Scottish public bodies

The Scottish Government has worked with the NCRLB to identify the requirements that will form the "initial baseline progression stage" under the Scottish Public Sector Cyber Resilience Framework. The Scottish Government will ask public bodies to achieve the following requirements to the following timelines:

■ **Key Action 2:** Have in place minimum cyber risk governance arrangements, by end June 2018.

■ **Key Action 3:** Ensure that public bodies that manage their own networks become active members of the NCSC's Cybersecurity Information Sharing Partnership (CiSP),in order to promote sharing of cyber threat intelligence, by end June 2018.

■ **Key Action 4:** Ensure they have in place appropriate independent assurance of critical cyber security controls by end October 2018. To support this goal, funding will be made available for public bodies to undergo Cyber Essentials "pre-assessments", by end March 2018.

■ **Key Action 5:** Implement as appropriate the NCSC's Active Cyber Defence Programme, which aims to make internet-based products and services safer to use, by end June 2018.

■ **Key Action 6:** Have in place appropriate cyber resilience training and awareness raising arrangements for individuals at all levels of the organisation, by end June 2018.

■ **Key Action 7:** Have in place appropriate cyber incident response plans as part of wider response arrangements, and ensure these align with central incident reporting and coordination mechanisms, by end June 2018.

C. Cyber security of supply chain and grant recipients

■ **Key Action 8:** Supply chain cyber security arrangements will form a key part of the Scottish Public Sector Cyber Resilience Framework. As part of due diligence, it makes good sense to ensure that other recipients of public money, such as grant recipients, also demonstrate that they take cyber security seriously. As part of work to develop the Framework, the Scottish Government will:

- develop a proportionate, risk-based policy in respect of supply chain cyber security (aligned appropriately with GDPR requirements), to be applied by public bodies in all relevant procurement processes. Industry partners will be consulted on a draft policy early in 2018, with a view to it forming part of the Scottish Public Sector Cyber Resilience Framework.
- develop guidance on the need for recipients of public grant funding to have in place appropriate, proportionate and risk-based cyber security arrangements. These requirements will align with the new supply chain policy and take effect alongside them.

D. Ensuring Scottish public bodies can access cyber security expertise and support

■ **Key Action 9:** To ensure that Scottish public bodies can access appropriate expertise in support of their work on cyber resilience, the Scottish Government will put in place an innovative Dynamic Purchasing System for Digital Services (including cyber security), by end October 2017.

E. Leadership and knowledge sharing

■ **Key Action 10:** To promote leadership and knowledge sharing, the Scottish Government will coordinate a Public Sector Cyber Catalyst scheme, under which a number of leadership bodies will commit to work towards becoming exemplars in respect of cyber resilience, helping identify common issues and solutions, and sharing learning and knowledge with the wider public sector.

F. Monitoring and Evaluation

■ **Key Action 11:** The Scottish Government will put in place a monitoring and evaluation framework to assess progress against this action plan and, once finalised, the Cyber Resilience Framework. A summary of the key actions different bodies should take, along with timelines, can be found at Annex A to this action plan.