G

AUDIT COMMITTEE REPORT

Subject: Cyber Security Update	**Purpose:** **For Approval** ☐ **For Discussion** ☒ **For Information** ☐
Prepared by: Hazel Robertson, Vice Principal – Finance and Corporate Services	**Date:** 18 May 2020

Purpose:
To update the Committee on Cyber Security recommendations for the College.

Linked to Strategic Goal 3: Provide a high quality College experience.

Executive Summary:

The attached paper prepared by the Head of ISLT outlines proposed recommendations towards the College's approach to cyber security. SLT approved the proposal to engage an organisation to carry out a Cyber Risk Technical Assessment and online training modules for staff on Security Awareness will also be progressed.

Recommendation:

The Committee to discuss and provide feedback on proposals.

Previous Committee Approvals:

For publication ☒	**For publication with redactions** ☐	**Not for publication** ☐

CYBER SECURITY

BACKGROUND

Cyber-attacks in their many forms is part of normal day life to organisations nowadays. The vast majority of which are dealt with through firewalls, security patches and anti-virus solutions meaning that the end users never have to experience any issues in their day-to-day operations. In fact most organisations are attacked every minute of every day.

Over the years, cyber-attacks have become more complex and targeted meaning organisations need to ensure they keep up to speed with the latest cyber-attack techniques and methods as well as the technology to assist with protecting their organisation.

Although we have improved many aspects of our security over the past 18 months by recruitment of staff with skill sets we were lacking, comprehensive patching schedules for our servers and network infrastructure as well as achieving our Cyber Essentials Plus accreditation I feel that this is an ideal opportunity to review our defences due to a various reasons.

- Our own cyber incident which occurred over the festive holidays
- The recent Ransomware attack at Dundee & Angus College
- More staff and students using online resources for learning and working. Office 365 being a prime example as well as the many online resources our teaching staff are using
- Cyber Essentials Plus accreditation – We are due to renew our accreditation in August
- Reinforce the importance of being cyber aware to our staff and student

As well as any technical development that may be required, it is just as important that we ensure our staff and students are educated as well. The majority of attacks on systems are caused by users clicking on an infected attachment in an email or a link taking them to a website.

PROPOSAL

I would like to recommend that we look at four main areas of cyber security that can assist the college with our defences to the ever growing threat.

General Security
This would review our system security such as patching, Anti Virus and access to internal systems. Critically it would also review our perimeter security and provide guidance on our firewalls and network configuration. This would be critical as we transition to using Office 365 more along with other online resources that authenticate to our in house systems.

Email Security Review
Again as we make more use of Office 365 and migrate our mailboxes to the cloud, a review would identify any weaknesses in our systems and processes to ensure we protect our data.

Data Backup Review
This is an area what ISLT have been looking at in some detail as our current solution is coming to end of life. A review of any new solution would not only take into consideration our current technical and security requirements but also our future requirements.

End User Training
As previously mentioned, it is imperative that we compliment any investment into our defences with end user training and education to ensure they are aware of the dangers presented to them everyday and the red flags to look out for.

SOLUTION

To assist with achieving our Cyber Essentials Plus accreditation last year we worked closely with our security partners 'Barrier Networks' and I would propose we enlist them in a project which will assist us achieving the actions outlined above.

Cyber Risk Technical Assessment
The proposed Cyber Risk Technical Assessment will help cover three of our action points in one engagement. This would provide detailed feedback on our general security, email security as well as a data backup review.

The purpose of the CRTA is to help the College identify any areas where cyber security related risks reside within our specific technology architecture. These risks can be related to anything from internet facing websites, insufficient USB removable media controls and email security. The Email security being important as that is where the breach over the festive period originate. The ransomware attack at Dundee & Angus College is also believed to have originated from an email.

The CRTA would involve information gathering to enable the consultant to acquire all of the details that they need to identify where cyber risk may be present. During the stakeholder interview phase Barrier Networks conduct short interviews with senior business stakeholders so that they can understand our business operations better. Understanding how we process data and why that data is important to your business.

The technical review is conducted by one of their experienced and qualified security architects and provides us with an end-to-end check of the controls that should be in place. The checks they perform are aligned to standards such as PCI DSS and the NIST CSF, and also industry best practice. The hands on review helps identify features, which are not configured properly, and provides recommendations on how to improve the security policies deployed, which helps us increase the effectiveness of your existing security investment.

Once the Information Gathering phase is completed, our consultant will spend time reviewing everything so that we can identify where cyber risk is present. The consultant will document all of the risks identified in the report and then use the business context gained to rate the impacts, and to prioritise them for remediation, based on what is important to your business.

Cost for the CRTA would be £5000 + vat, plus any additional work which comes from the review.

End user Training (Security Awareness)
They are many training options available to staff including some of our compliance modules as well as a multitude of online material. Barrier suggested that investing in security awareness training would help with any future reports to the ICO. Barrier organised two demos of a solution called Knowb4, one with myself and the other with member of the HR and Development team. The feedback from us both was positive. Further discussion to be had with SLT/Exec if this solution to be implemented.

Cost for KnowB4 One Year Subscription would be £4,440 + vat

Working with Barrier Networks on their proposed solutions, this would enable us to complete the review into the four main areas identified above. Allowing us to identify the areas we need to focus our attention, firstly to identify any quick wins we can achieve but also to work on a longer term strategy which may require some additional investment.