REGIONAL BOARD REPORT

Subject: Cyber Resilience	**Purpose:** **For Approval** ☐ **For Discussion** ☒ **For Information** ☐
Prepared by: Peter D Smith, Vice Principal – Finance and Resources	**Date:** 19 October 2017

Purpose:
To consider the impact of the Scottish Government's proposals with regard to cyber resilience in the public sector.

Linked to Strategic Goal 5: Build Sustainability.

Executive Summary:

Following recent high profile failures, Board members will be well aware of the issues surrounding cyber security and cyber resilience. In August 2017, the Scottish Government issued a consultation on a proposed action plan and best practice guidelines for Scotland's public sector. The full consultation is found here: -

https://blogs.gov.scot/cyber-resilience/2017/08/08/draft-public-sector-action-plan-and-best-practice-guidelines-views-welcome/

Borders College's response is attached.

Many public sector organisations had similar concerns and these have been incorporated into further drafts of the Plan. A summary of the changes is also attached and I can provide Board members with copies of the updated drafts on request.

In reviewing our own current capabilities, we believe we already have in place considerable measures appropriate to our organisational profile: -

- Borders College uses Sophos Endpoint security. This runs on all PC's in the college and it is updated automatically with the latest virus signatures.
- Microsoft security patches are deployed automatically from a central server and kept up to date.
- Servers have Sophos checking stored files for viruses and are updated automatically with the latest virus signatures.
- Proxy server access to the internet is via a proxy server that filters content and blocks download of those types of files designated as posing a risk.
- Users are not allowed to install software on college machines as they do not have admin rights - this also stops viruses from trying to install code.
- There is a firewall in place that has an extensive set of rules to block unwanted content. As this is a single point of failure this is being replaced with 2 firewalls with automatic fail over.
- The network is segmented so that if a virus did get through it reduces the spread and makes it easier to find.
- Sharing permissions are monitored to reduce the spread of viruses and make them easier to track.

- There are extensive sets of backup that can be used to recover from attack, these have been tested.
- JISC monitors incoming and outbound internet traffic and will proactively block attacks.
- Wi Fi system checks devices connecting to make sure they are acceptable and also for rogue devices and access points.
- Switches look for traffic storms and will automatically shut down ports that are injecting unexpected traffic.
- Systems monitor for unexpected traffic increases at switches, Wifi, Firewall, and will close down this extra traffic automatically. There is also monitoring software on these systems that reports on any suspicion activity and sends an e-mail to the server team.
- We have undertaken staff awareness sessions to ensure they are aware that often it is human action or inaction that may inadvertently provide the initial security breach.

The measures above provide good assurance that Borders College is well equipped to protect itself from and respond to cyber threats; however, implementation of the best practice guidelines will undoubtedly increase the level of resource required to demonstrate compliance and meet monitoring arrangements, particularly as the guidelines propose mandatory accreditation to Cyber Essentials Plus standard.

Recommendation:
Board to discuss the implications on Borders College of the Scottish Government proposals and cyber resilience more generally.

Previous Committee Approvals:
n/a

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

Cyber Resilience Consultation Update

The comments we received from public sector organisations on the original draft suggested a high level of support for the aims of the action plan and much of its content. The key challenges identified were: (i) **Timelines** – the majority of respondents felt the timelines set out in the draft were unachievable; (ii) **Resources** – many organisations had already allocated budgets for this year, and had limited resources available to implement the plan before end FY17/18; and (iii) **Duplication** – some of the more sophisticated bodies argued they already had accreditation in place, and are working to a range of different standards and guidelines that could be duplicated by some of the draft action plan's requirements.

In addition, there have been some key developments at the UK Government level that have impacted on the draft proposals. These include clarity that detailed guidance on the high level cyber security principles that will form part of UK implementation of the **EU NIS Directive** will not be made available until **January 2018**, as well as a proposal to introduce a new **Technology Security Standard** for all UK Government Departments under the Security Policy Framework shortly.

To take account of these issues, and informed by further discussions with key partners, we have made some key changes to the earlier draft. While the core of the actions remain the same or similar, the key changes are:

- Rethinking the best practice guidelines, and instead committing to developing a **Cyber Resilience Framework** for the Scottish Public Sector that takes account of developments at the UK level, and aligns more closely with NIS and the wide range of standards that Scottish public bodies are currently working to.
- Adding in some further baseline requirements in respect of **governance** and **incident response**.
- Clarifying the position on **Cyber Essentials/Plus certification**, including by saying that the boards of public bodies can decide whether to seek Cyber Essentials "basic" or "plus" based on their assessment of risk, and the extent to which their appetite for independent assurance around the five critical controls is met by alternative accreditation.
- **Extending timelines** to be more realistic, whilst ensuring that the urgency of addressing the increasing cyber threat is taken into account.

Questions for Scottish public sector organisations on the draft public sector action plan and draft best practice guidelines on cyber resilience

Please provide comments on the draft action plan and the draft best practice guidelines on cyber resilience in line with the following questions.

Question 1: To provide important context, please give an overview of your current arrangements for cyber security. In particular, please provide details of:

- any relevant accreditations held, or standards met, by your organisation
- current board level, governance and risk management arrangements for managing the cyber threat in your organisation
- any ongoing programmes of work on cyber security in your organisation
- the current level of resource you devote to cyber security in your organisation.

Answer to Question 1

At Borders College, our Board monitors our actions to counter cyber threat as part of our Strategic Risk Register. The Audit Committee receives regular updates on the current position, and we undertake internal audit exercises to ensure compliance. Our ISLT Strategy Committee, as part of Senior Leadership Team, is responsible for agreeing annual investment plans, including in response to cyber threat. At operational level, there is an incident response plan and business continuity plan which are subject to regular testing. Staff and student awareness and training sessions are held regularly.

We are in the final stages of an ICT infrastructure replacement programme, reflecting best practice across switching, w-ifi, IP telephony, firewall and virtualised servers. Security and monitoring have been built into the new systems in line with current best practice. The design and layout has been changed to improve security. There is greater segmentation to eliminate the likelihood of a single point of failure. Software, firmware and patches are kept up-to-date.

Responsibility for cyber security rests principally with the Head of ISLT and Server Support Analyst from within the Information Services Team. This small team consists of only 8 individuals, so no-one is exclusively dedicated to cyber security.

Question 2: Please give your views on the draft public sector action plan and best practice guidelines. We would particularly welcome views on:

- Whether there are any key omissions from the plan
- Whether there is likely to be any unnecessary duplication as a result of the plan
- Whether you believe the plan, if implemented, would make a significant difference to levels of cyber resilience among Scotland's public bodies.

Answer to Question 2

We do not believe there are any key omissions.
We have no views on whether there may be unnecessary duplication.
Without a detailed knowledge of other bodies' current cyber resilience it is not possible to comment.

Question 3: Please identify any key implementation challenges for your organisation in respect of the draft public sector action plan and best practice guidelines.

Answer to Question 3

Borders College, as an education provider, and as a provider of shared ICT services to Heriot-Watt University's School of Textiles and Design, has a number of challenges in providing a secure data network while also providing access to a wide-ranging group of stakeholders. Allowing for the concept of Bring-Your-Own-Device (BYOD) and the use of media for examinations, it is not possible to block all media without this having a major impact on students and making use of the facilities impractical. We therefore must take a proportionate view in balancing access and risk exposure.

The level of resourcing required may also present a challenge to a small organisation with a small IS team. It is vital to recognise that implementation must be proportionate to each organisation's needs and purpose. Even the cost of accreditation may be prohibitive.

We would welcome the proposed provision of practical support as set out in the draft plan.

Question 4: If you are a public sector organisation that is not subject to the Scottish Public Finance Manual, please indicate whether you would be in favour of adopting the recommendations set out in the draft action plan and best practice guidelines to ensure alignment with other public sector organisations.

Answer to Question 4

n/a – we are subject to SPFM

Question 5: Please indicate whether you would be willing in principle for your organisation to become a public sector cyber catalyst, in line with the description set out in the draft action plan at Key Actions 6 and 7. (Please note: due to practical considerations, not all organisations volunteering are likely to be selected as cyber catalyst organisations)

Answer to Question 5

Yes, subject to the support noted under Key Action 7 being made available to effect any changes.