Meeting Date	**09 July 2020**		**Agenda Item**	**2.2**
Report Title	**Cyber Security Update Report**			
Report Author	Gareth Ayres (Cyber Security Manager)			
Report Sponsor	Matt John (Associate Director of Digital Services)			
Presented by	Carl Mustad (Head of ICT Operations)			
Freedom of Information	Open			
Purpose of the Report	The purpose of this paper is to provide an update on the ongoing Cyber Security Risk faced by the Health Board; and the recent measures taken to help address the risk.			
Key Issues	Whilst the Cyber Security risk remains high, significant progress has been made to improve Cyber Security at SBUHB through the; • establishment of a Cyber Security Team • Adoption of new National and Local cyber security tools • Preparation for compliance with the European Regulation - Network & Information Systems Directive (NIS-D) and Cyber Essential+ standards. • Ongoing work to update legacy systems to new supported versions. Reports suggest that two-thirds of Cyber Security incidents are the direct result of employee behaviour. Whilst there is a Cyber Security training module in ESR, this has not been made mandatory.			
Recommendations	Members are asked to: • **NOTE** the significance of the cyber security risk faced by the Health Board • **NOTE** the progress that has been made to mitigate against the risk • **NOTE** the agreement by Senior Leadership Team, in principle, for Cyber Security Training to be made mandatory. A further paper for approval, describing the implications for the workforce, will be submitted to a future SLT meeting.			
Specific Action Required ***(please choose one only)***	**Information**	**Discussion**	**Assurance**	**Approval**
	☐	☐	☒	☐

CYBER SECURITY UPDATE REPORT

1. INTRODUCTION

Swansea Bay University Health Board is making increasing use of digital services to enable all areas of the organisation to work efficiently, securely and recently; increasingly remotely. The confidentiality and integrity of our data, and availability of our digital services has a direct impact on our staff's ability to perform and ultimately on patient outcomes; as well as our reputation and the confidence of the public in the services we offer.

There is a High Level Cyber Security risk on the Health Boards Risk Register. The goal is to reduce the risk and impact as far as realistically possible given the ever present threats. This report will outline the progress made so far, future plans, and recommendations.

2. BACKGROUND

The number of cyber security incidents is at an unprecedented level and health is a known target. The health board has significantly increased digital services (users, devices and systems) and therefore the impact of a cyber-security attack is much higher than in previous years.

The recent pressures on Health to deal with the COVID-19 epidemic has resulted in even more targeted and sophisticated attacks; exploiting the situation and applying unique pressures on NHS staff to disrupt healthcare in order to extort financial gains.

SBU Health Board faces a range of cyber-attacks daily, both targeted and opportunistic. The high profile WannaCry attack from 2017 highlighted the impact a successful attack can have across the NHS, with cancelled appointments and an estimated £92M cost. Emails targeting our staff are a common attack method, and there are several national and local measures which address this threat very well. However, inevitably, some malicious emails do get through the system and the consequence of these can range from interruption to an individual and in the worst case scenario, interruption to the whole of the organisation.

A number of cutting-edge technologies to monitor, detect and proactively stop cyber-attacks are implemented in SBU. These tools are complex to use and require dedicated resources and immediate attention when an event occurs. The newly established Cyber Security Team provides a security operations function to make best use of these tools, as well as support staff and work with national colleagues as a wider network to prevent cyber-attacks and data loss.

Following cyber-attacks on Health and other public sector bodies, European Union Regulation was introduced in 2018 and Network & Information Systems Directive (NIS-D) was adopted by the UK Government. Failure to protect the network and information systems, which could result in interruption in services and loss of data, can result in fines of up to £17m (in addition to fines resulting from data loss in the General Data Protection Regulation – GDPR).

The Welsh Government is the Competent Authority under NISD and the Health Board will be expected to report in line with WG requirements. The management arrangements and audit processes are yet to be defined.

In preparation for compliance a number of technical and governance controls have been put in place, or planned as detailed in the remainder of this document, and expanded upon in Appendix 1.

3. GOVERNANCE AND RISK ISSUES

There are a number of cyber security risk that all organisations have to deal with. Below are the most common areas that the health board faces on a daily basis along with the tools and processes employed to mitigate against them.

Email and People

The Health Board receives a significant number of external emails every day. Some of these are malicious emails either sent speculatively to groups of users, or are more sophisticated and target relevant staff, such as asking for payments for companies that the organisation has legitimate dealings with but with spurious bank details.

Training users to detect, delete and report these malicious emails is vital to improving our Cyber Security Awareness across the whole organisation. National tools are in place to ensure the vast majority of these emails are deleted at source, however it is inevitable that some get through the system, with the more sophisticated malicious emails tending to be in that category.

The Health Board has procured a new solution to enable the organisation's workforce to be tested for their ability to notice malicious emails. Anyone who clicks on a link in an email asking for account or payment details will be notified that they have done this and targeted for training.

Directly targeting employees is the most common way for cyber criminals to successfully exploit organisations. A recent report from a leading software security provider (Symantec) found that 71% of all targeted attacks started with malicious emails. Supporting our staff to help identify these common threats through mandatory and targeted training will have a significant positive impact in defending against a cyber security attack.

Old Software and Devices

The importance of keeping software and devices up to date is essential to defend against cyber attacks. The Wannacry attack (mentioned above) was successful because the NHS was running old and out of support computer systems.

Significant progress has been made across the Health Board to keep software and devices up to date with the latest security updates and features. An in-house developed Server Patch Management system has been implemented to show live information on compliance levels with up to date software for the Health Board servers.

By using local security/admin tools to track and understand software installed on user devices (laptops/desktops/iPads), those devices can then be updated or retired appropriately. These tools are also in place to either update old software (cyber risk) or remove as appropriate. Devices which are nearing end of life (circa 5-7 years old) are scheduled to be replaced so that our devices across the estate are always covered by maintenance and support agreements and run the latest software. Digital working groups covering different areas (computers, networks and computer systems) are set up to address this and progress/requirements are reported to the Digital Service Management Group with a subsequent a priority list submitted to the capital investment group.

There are however software and devices in use which cannot easily be replaced or updated for a variety of reasons (for example systems linked to specific medical equipment), and mitigations are put in place to minimise the risks associated with those systems and devices. Controls such as only allowing computer systems to communicate with the devices it needs, rather than allowing access to our entire network. As well as methods to monitor any suspicious behaviour using the advanced tools used by the Cyber Security team.

Network Threats

As demonstrated by Wannacry, some cyber threats can be spread via vulnerable devices internally in NHS Wales and externally as well. The Cyber Security Team have a number of tools that help protect against and detect these threats. The Health Board is protected by local Firewalls, as well as National Firewalls which block unwanted network connections from the internet. Advanced networking monitoring tools are also used reactively and proactively to identify potential threats or suspicious behaviour.

The events and logs from a number of IT core systems are collated in one place for the Cyber Security Team to monitor for unusual or suspicious activity, in order to limit the impact of any possible cyber incidents. Having continuous monitoring and a rapid response to cyber incidents is vital to ensure continuously effective cyber security.

External Partners

The Health Board has close working arrangements with numerous partners including other NHS organisations, private companies and other public sector bodies. There are often special network and data sharing arrangements with these partners, and this represents a very real risk if they suffer a cyber security incident. This could result in our data being lost, but also act as an avenue for an attacker to target our systems and users.

The advanced tools highlighted above are used to control and monitor access by third parties, but an inevitable part of these relationships is a shared cyber risk. The Cyber credentials of external partners are checked by the Cyber Security Team to ensure they meet the Welsh Government and the Health and Social Care Network requirements for access. A new Cyber Security Impact Assessment document is now used as part of the procurement process to help capture the Cyber Security assurance third parties can provide before engaging with them.

Further information on the controls in place and more detail on the tools and processes to protect the organisation against cyber attacks is in attached in the appendix.

4. FINANCIAL IMPLICATIONS

The Health Board and Welsh Government has recognised the increasing threat posed by Cyber Security risks, and a new Cyber Security Team has now been established, consisting of:-

- Band 8a Cyber Security Manager
- Existing Band 7 Cyber Security lead
- Additional two Band 6 posts as Cyber Security Specialists.

It should be noted that the Band 6 posts are currently funded by Welsh Government. Welsh Government indicated that funding will remain for the 2 posts for an initial 3 years (at least until 21/22) and therefore the roles were recruited to permanently, within SBUHB and other organisations. However, funding for 20/21 has not yet been confirmed. WG are currently working through the effects of COVID-19 on the National Digital Prioritisation Fund before confirming allocations.

Welsh Government funding for cyber security has also allowed for the procurement of two cyber security tools which have ongoing revenue consequences associated with them:

- **Network Monitoring** – Two products called Cisco StealthWatch (5 year contract) and Firewalls (3 year contract) have been procured and funded by WG for use at the Health Board. These product allows proactive and reactive incident response for cyber incidents to mitigate against local Network Threats (explained above). There will be ongoing revenue implications. Welsh Government have indicated that revenue will be provided for 3 years. (Approx £92,000 inclusive of VAT per annum)
- **Scam Email Simulation and Training** – A solution from Metacompliance has been procured with the WG funding for our Health Board on a 1 year recurrent revenue basis, that will allow for the ongoing testing and training of Cyber Awareness for our local staff (see **Email and People above)**. Welsh Government have indicated that revenue will be provided for 3 years. Cost £38,520 inclusive of VAT per annum

Therefore, provided WG commit to the original outlay, costs for these resources and tools will be covered until end of 21/22. Digital Services and Finance colleagues will escalate with WG colleagues as required over the next period.

This report shows the excellent progress made to address the cyber security risks that the Health Board faces. There have been a number of attacks, and more recently related to COVID to further entice our staff to click on “important” links, which have been dealt with locally and nationally. These are threats that the Cyber Security team deal with on a daily basis and shows that the cyber security risk is real and the number of incidents continue to rise.

The establishment of a professional cyber security team and adoption of advanced Cyber Security tools is essential for dealing with these threats. The team was effectively fully established from February 2020 and are already utilising the advanced cyber security tools to protect the organisation against cyber attacks.

The risk of cyber security attack which exploits our staff remains high. The workforce needs to be fully aware of the cyber security risks facing the organisation to combat targeted attacks effectively. In order to address this, it was recommended to the Senior Leadership Team (SLT) in June for Cyber Security training to be made mandatory. SLT agreed in principle that Cyber Security training should be mandatory but also highlighted concern regarding any potential risk to mandatory training compliance as a whole. An action was recorded for Cyber Security Leads to provide a further detailed proposal regarding Cyber Security Training and implications for the workforce at a future SLT meeting.

Whilst considerable progress has been made across the HB, the requirement to achieve and maintain compliance with NISD will also require considerable resources and this plan will be developed in due course following confirmation of requirements from WG. The continuous support and development of the Cyber Security team and the local and national tools is essential to maintain safe services.

5. RECOMMENDATION

Members are asked to:

- **NOTE** the significance of the cyber security risk faced by the Health Board
- **NOTE** the progress that has been made to mitigate against the risk
- **NOTE** the agreement by Senior Leadership Team, in principle, for Cyber Security Training to be made mandatory in principle. A further paper for approval, describing the implications for the workforce, will be submitted to a future SLT meeting.

Governance and Assurance		
Link to Enabling Objectives ***(please choose)***	**Supporting better health and wellbeing by actively promoting and empowering people to live well in resilient communities**	
	Partnerships for Improving Health and Wellbeing	☐
	Co-Production and Health Literacy	☐
	Digitally Enabled Health and Wellbeing	☒
	Deliver better care through excellent health and care services achieving the outcomes that matter most to people	
	Best Value Outcomes and High Quality Care	☐
	Partnerships for Care	☐
	Excellent Staff	☐
	Digitally Enabled Care	☒
	Outstanding Research, Innovation, Education and Learning	☐
Health and Care Standards		
(please choose)	Staying Healthy	☐
	Safe Care	☐
	Effective Care	☐
	Dignified Care	☐
	Timely Care	☐
	Individual Care	☐
	Staff and Resources	☒
Quality, Safety and Patient Experience		
N/A		
Financial Implications		
Welsh government have indicated that the funding for the 2 band 6 posts and cyber security tools (£130K for tools) will be available for 3 years (2019-2022). However, this is not yet guaranteed and currently at risk.		
Legal Implications (including equality and diversity assessment)		
Regulatory compliance with the Network and Information Systems Directive (NISD). Failure to meet compliance or successful cyber-attack on the Health Board can result in fines of up to £17M.		
Staffing Implications		
As the plan for compliance with NIS-D is developed, any additional requirements for resources will be defined in the plan.		
n/a		
Report History	N/A	
Appendices	Appendix 1 – Detailed information on controls identified in high level risk	