Meeting Date	**30 July 2020**	**Agenda Item**	**3.5**
Report Title	**Cyber Security Update Report**		
Report Author	Gareth Ayres (Cyber Security Manager)		
Report Sponsor	Matt John (Associate Director of Digital Services)		
Presented by	Matt John (Associate Director of Digital Services)		
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. This paper has already been presented to Senior Leadership Team and Audit Committee.		
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.

NHS Wales receive around 1,000 emails per month that contain viruses or malicious content.

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.

In May and June 2020, a significant increase in the number of attempted attacks were detected on national security systems.

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 were funded by Welsh Government in 19/20. WG are currently working through the effects of COVID-19 on the National Digital Prioritisation Fund. We have been informed that they are unlikely to be in a position to fund those roles from this year onwards.

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

Digital Services and Finance colleagues are currently working through how to address the funding shortfall.

5. CONCLUSION

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 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.

6. 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. 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		
Digital Services and Finance colleagues are currently working through how to address the funding shortfall for resources and maintenance costs as referenced above.		
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	

Appendix 1 – Further information on controls, resources and systems in place to provide effective cyber security services within Swansea Bay University Health Board

The controls detailed in the high level cyber security risk consisted of the following actions:-

- **Recruitment of Cyber Security Team**
- **Adopt national tools to highlight vulnerabilities and provide warnings when potential attacks are occurring.**
- **Ensure existing tools provide effective protection against potential Cyber Security attacks**
- **Ensure malicious emails coming into Swansea Bay through NHS Wales gateway are acted on efficiently and effectively**
- **A strong patching regime established to protect against any known security vulnerabilities.**
- **Effective response to alerts raised from the Anti-virus system.**
- **Ensure old systems that are no longer supported are upgraded to supported versions to mitigate against security vulnerabilities.**
- **Rollout of a Cyber Security training module to raise awareness for staff, this is essential as staff are the biggest risk for any cyber security attack.**

1. Recruitment of Cyber Security Team

At the time this risk was submitted, the Cyber Security resource was a single Band 7 WTE.

A new Cyber Security Team has now been established:-

- 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, and in addition to the Band 8a post are supported at risk by Digital Services).

This has allowed for the setup of a Security Operations Centre to be established in a dedicated environment for the Cyber Team to monitor cyber events in real time and adopt a proactive approach to real time security alerting and take appropriate mitigating actions and onward reporting. This is already providing benefits to the organisation in terms of identifying risks and providing rapid response to those risks.

The Cyber Security Team at Swansea Bay has strong partnership links in place. It works closely with a number of national groups as well as the Cyber Security Team at NWIS through the Operational Service Security Management Board (OSSMB). The team also has membership of the National Cyber Security Centres (NCSC) Cyber Information Sharing Partnership (CiSP) as well as the welsh WARP and Local Resilience Forum who have representatives from the Regional Organised Crime Cyber Unit TARIAN.

2. Adopt national tools to highlight vulnerabilities and provide warnings when potential attacks are occurring.

Progress has been made with the adoption of national tools provided by NWIS (Welsh Government Cyber Security Funding). The resources in the newly established team are essential in providing expert knowledge and ability to act on any issues identified.

- **Security Incident and Event Management system** (**SIEM**) – This allows for centralised logging and alerting of suspicious events across all systems and networks. Local installation has been implemented, with health board system cyber events feeding into the SIEM. Feeds from the health board Anti Virus and End Point Protection system, the SBU Smoothwall Web Proxy (Internet Filter) and the local instance of the national Active Directory which collects information on failed login attempts which could be an early warning that there is a potential cyber attack by malware that is trying different passwords to login to a system. This will provide a dashboard for security monitoring to ensure visibility of potential cyber threats and appropriate action taken by the newly formed Cyber Security team. Training for Cyber staff on operational use of the SIEM was scheduled for March 2020 but Covid digital activities across NHS Wales means that this was postponed and rearranged for a date in July via Teams. The team in conjunction with Security resources in NWIS monitor events on a daily basis. The training will ensure staff have the up to date knowledge to make the best use of the system in Swansea Bay.

- **National Vulnerability Management System** (**Nessus**) - This is a system which scans devices attached to the network for known security issues and report on the severity of them, This has recently been implemented at SBU and training for Cyber Security staff completed on May 21st 2020. This process has started with the Server team as a proof of concept.

3. Ensure existing tools provide effective protection against potential Cyber Security attacks

A number of local tools and national systems have been in place for a number of years to protect against malicious attacks. These include:

Local System	**New Activity following formation of Cyber Security Team**
Anti Virus and Endpoint Security – Kaspersky Endpoint Security renewed in 2020 which provides the Anti-Virus protection for desktop, laptop and server computers. In addition, Endpoint Security Management which forces encryption of USB memory sticks to	Cyber Team have a dashboard displaying events and proactively manage this.

protect data. Kaspersky are recognised as one of the Leaders in this field.	
Filtered Web Access – Web traffic from all devices on the HB network is sent via the Smoothwall Web Filter which provides controls around which user groups can access which content types and provides additional protection to block access on known malicious sites.	Rule sets are actively monitored and any sites highlighted as risks are actively blocked. This has been of particular importance during the COVID-19 pandemic to stop staff inadvertently accessing fake sites.
Secure File Sharing Portal – This is used to securely transfer files to people outside of the organisation to protect against confidential and person identifiable information getting into the wrong hands.	Cyber team have improved the process to securely transfer confidential and Person Identifiable documents. The process is much quicker than previously possible with a single resource and helps mitigate against work around solutions which could inadvertently result in confidential information getting in the wrong hands.

4. Ensure malicious emails coming into Swansea Bay through NHS Wales gateway are acted on efficiently and effectively

The newly established Cyber Security team have developed a process to act upon malicious emails which have inadvertently come through the national email filter. These are daily events and without the new resources, would have taken substantially longer, especially when previously there was only one resource who could be training or in a meeting.

5. A strong patching regime established to protect against any known security vulnerabilities.

The health board computer devices have excellent compliance levels with Microsoft patching. The following systems are in place to ensure compliance levels are maintained.

System	**New Activity following formation of Cyber Security Team**
Asset Management – SNOW asset management software has been deployed to health board computers and provides hardware and software inventory. This provides detail on the device hardware, software installed and who has used it. This is essential to highlighting any potential software	**Secure Managed Device Review Group** A cross team working group with Cyber Team, Infrastructure Team and Desktop Team to review the managed device estate and the plan to bring all devices to a position they are running up-to-date **operating systems** and supported hardware. SBU Service Delivery Manager chaired the All Wales Device

vulnerabilities. Microsoft SCCM is also used in conjunction with SNOW to provide updates to protect against software security vulnerabilities.	management Group to ensure Windows 7 (non supported January 2020 – extended to 2021 following the new licence agreement with Microsoft) devices were upgraded to Windows 10. Nationally SBU are leading in this across Wales **A High Risk Software Review Working Group** – Recently setup collaboration with Cyber Team and Desktop Team to perform weekly review of high risk software installed on managed devices. Compliance levels are monitored and reducing the number of agreed software for essential needs only ensure that programs are updated regularly to reduce the risk of a cyber attack on old vulnerable software. Given the amount of software installed, this work is ongoing to reduce numbers. Weekly meeting.
Server Patch Management Monitoring– Ensuring latest software updates are applied is essential in defending against security attacks on vulnerable systems. An in-house developed Server Patch Management system has been implemented to show security patch levels for the Health Board servers. A simple dashboard shows compliance levels with latest releases. This is in direct response to the national recommendation from the All Wales Stratia Report.	**Secure Infrastructure Review Group** A cross team working group with the Cyber Team and Infrastructure Team to review servers and services are using the latest supported operating systems and software.

6. Effective response to alerts raised from the Anti-virus system

As detailed in section 3.

7. Ensure old systems that are no longer supported are upgraded to supported versions to mitigate against security vulnerabilities.

There are a number of older systems running on software that is no longer updated mainly due to departments not implementing the latest versions. A plan will be developed in order to move these to supported versions. Funding for a fixed term post has been requested from capital 2020/21 but has stalled due to Covid activities. There will inevitably be further costs which will need to be funded further as identified by the fixed term post. From a Governance perspective, the Digital Service Management Group has

been established to ensure departmental representatives manage their systems in a safe and secure manner.

8. Rollout of a Cyber Security training module to raise awareness for staff, this is essential as staff are the biggest risk for any cyber security attack.

A national Cyber Security Training Package has been deployed locally, through ESR which will offer a number of modules on improving awareness around Cyber Security.

Mandatory adoption of this training package **is not in place yet**. Until this is made mandatory and the training module has been completed by all staff, the cyber security risk associated with staff ill equipped to notice phishing or fraudulent emails remain at a high level. This has been taken to the mandatory training board but no agreement has been reached to adopt this essential Cyber Security training/awareness course.

In addition, a **Phishing** (basically a hacker's phrase for conning an online user, usually through email) **Simulation Campaign and Targeted Training software package has been procured from** Welsh Government Cyber Security funding (Metaphish). This allows the Cyber Team to perform a simulated phishing attack and depending on the staff response (clicks on a malicious link or not) provides a dashboard view on how many staff are aware of phishing emails and conversely who needs additional training to ensure they don't get exploited when real risk phishing emails come in. The training material complements the training Cyber Security module within ESR but emphases the risk of phishing emails. to raise awareness of Cyber Security risks and provide essential learning to mitigate against those risks.

9. Additional Cyber Security tools procured to enhance protection

In addition, the following cyber security systems are being implemented. These were funded by Welsh Government to enhance Cyber Security defences based on local needs.

System	Additional Protection
Network Monitoring and Visibility	Procured Cisco Stealth Watch (Welsh Government Cyber Security Funding) to allow real time monitoring and provide early warning for suspicious activity of the health board computer network, as well as retrospective analysis with the use of advanced machine learning. Early warning is critical in order to stop further potential damage caused by malicious attacks and limit the impact on availability/data loss.
Local Firewalls	Procured Cisco Firepower next generation firewalls (internal) to complement the Cisco Security Centre firewalls which protects the network traffic entering and leaving the health board. These provide additional internal security protection.

A Secure Networking Group has been established. A weekly review with the Network and Cyber Security Team to review network security. This group provides expert knowledge in terms of the management of the newly procured solutions and effective proactive management of any network related security alerts from existing and new security tools.

The Health Board also has an internet link, an annual independent vulnerability check is made to ensure services are secure and mitigates against unauthorised access.