GIG CYMRU NHS WALES | Bwrdd Iechyd Prifysgol Hywel Dda University Health Board

PWYLLGOR ADNODDAU CYNALIADWY
SUSTAINABLE RESOURCES COMMITTEE

DYDDIAD Y CYFARFOD: **DATE OF MEETING:**	28 October 2021
TEITL YR ADRODDIAD: **TITLE OF REPORT:**	Update on Risk 451: Cyber Security Breach
CYFARWYDDWR ARWEINIOL: **LEAD DIRECTOR:**	Huw Thomas, Director of Finance
SWYDDOG ADRODD: **REPORTING OFFICER:**	Anthony Tracey, Digital Director

Pwrpas yr Adroddiad (dewiswch fel yn addas)
Purpose of the Report (select as appropriate)

Er Sicrwydd/For Assurance

ADRODDIAD SCAA
SBAR REPORT

Sefyllfa / Situation

This purpose of this report is to update the Sustainable Resources Committee on the Health Board's ongoing Cyber Security compliance activities, consideration of new UK legislation, and the related Corporate Risk 451: Cyber Security Breach.

In 2017, the then NHS Wales Informatics Service (NWIS) outlined their Welsh Cyber Assurance Process (WCAP). The intended outcome of this all Wales funded initiative was to provide assurance to the Welsh Government, Audit Office Wales, and external suppliers, that connection to the NHS Wales network and the services it provides is secure, and to enable the creation of locally focussed action plans to improve security as a result of the "WannaCry" cyber-attack. As a result, Risk 45: Cyber Security Breach was drafted.

Cefndir / Background

A strong cyber awareness culture is one of the best defences against cyber-attacks. Regulations such as the Network and Information Security (NIS) Directive and the General Data Protection Regulation (GDPR) will increase the burden on organisations to ensure they have effective cyber-security strategies and culture in place, in addition to robust controls and policies, to prevent and remediate attacks.

In October 2017, Stratia Consulting was commissioned by Velindre NHS Trust, on behalf of NHS Wales, to carry out external cyber security assessments for its organisations. For each organisation, a cyber security assessment report and security improvement plan (SIP) were produced. This review sought to provide the Hywel Dda University Health Board (HDdUHB) with assurance regarding the progress in implementing its security improvement plan.

The security assessment for HDdUHB was undertaken in January 2018. The outcome of this assessment was the publication of a local HDdUHB summary report, the NHS Wales External Security Assessment - HDdUHB Report and Improvement Plan.

Over the past 3 years, the Digital Team has been working with Digital Health and Care Wales (DHCW) to enact the action plan to provide assurances to the Health Board that, in the event of further cyber-attacks, HDdUHB and the wider NHS in Wales would be secure. Work undertaken to date includes protecting the Health Board's computers, networks, software programmes, and data from unintended or unauthorised access, change or destruction via the internet or other communications systems or technologies.

Consideration of Cyber Security should be within the same realm as Information Governance. The penalties for non-compliance are similar to those for a data/information breach and therefore, the Health Board should consider establishing a Cyber Resilience Team to work with DHCW to ensure that robust processes are in place. NHS Wales is only as secure as its weakest link.

Asesiad / Assessment

The Stratia Report highlighted where the Health Board was compliant, where shortfalls exist, and included a SIP providing recommendations to address any issues. Feedback from Stratia was on the whole positive. The report illustrated that although the Health Board had passed the assessments below, improvements could be implemented:

- E-mail system passed the security tests
- Desktop PCs had very good protection status and all tests were passed
- Internet link and MobileIron passed all the security tests

Concerns were raised regarding:

- a lack of vulnerability scanning tools
- a lack of resources, from a software and staffing perspective, to undertake patching
- the existence of legacy software, which no longer receive security patches or software updates

As a result of the report and lessons learned from the cyber-attacks, a number of key activities were considered essential and formed part of the mitigations for Risk 451. These lessons learned and their current status are detailed below:

- **Vulnerability Scanning -** All modern software contains vulnerabilities; either software defects that require patches to remedy, or configuration issues that require administrative activity to resolve. For this reason, the Health Board should have a vulnerability management solution, which would enable the Health Board to discover what vulnerabilities are present within its Information and Communication Technology (ICT) estate on a regular basis and to act on these vulnerabilities.
  Status: *Complete - Implementation of vulnerability scanning solution has been completed and scans are underway on a regular basis. However, the scanning is only one element and there is a current challenge to fix the vulnerabilities identified.*
- **Patch Management -** Exploitation of known vulnerabilities in software remains the greatest risk of a security incident occurring, which can affect the Health Board. In order to protect the Health Board, security patching is used to ensure the systems are updated accordingly and protected from known cyber-attacks as vendors such as Microsoft release security updates.
  Status*: Complete - Implementation of new patching framework for desktop, server and managed equipment estate has been adopted.*
- **Maintenance Windows -** In ICT and systems management, a maintenance window is a period of time designated in advance by the technical teams during which time preventative maintenance may be performed. This maintenance typically involves the

installation of security patches or software updates that require a system reboot and therefore could cause disruption to services.
Status: *The implementation of new patching framework for desktop, server and managed equipment estate has been adopted, which has required agreed maintenance windows with the Information Asset Owners.*

- **Penetration Testing -** Whilst vulnerability scans outlined above would highlight risks across the network, penetration tests involve a security specialist testing the defences in place, therefore simulating a cyber-attack. By undertaking penetration tests annually, or after a major system change, the Health Board can receive assurance that the security measures in place are effective and relevant.
Status*: Work has commenced for implementation of a Security Incident Event Management Solution, which includes the adoption of regular penetration testing.*
- **Anti-Virus Enhancements -** The Health Board has a well-established Anti-Virus platform using Sophos technologies. During the recent WannaCry outbreak, the platform successfully detected and cleaned the infection from a number of computers. This solution automatically updates virus definitions on ICT managed equipment and ensures regular scans are undertaken to identify cyber security threats.
Status: *Specific module to protect the Health Board against a zero-day ransomware attacks is being developed with an anticipated completion date of December 2021.*

The lack of pace on delivery has been recognised by the Information Governance Sub-Committee, which can be attributed to the lack of dedicated Cyber Security resources and challenges with recruitment. This has improved with the appointment of a Cyber Security Specialist in May 2021 and a second Cyber post is currently undergoing employment checks. However, there is a need for additional resources to create a Cyber Resilience Team for the Health Board. Following the appointment of the Cyber Specialist and with support from specialist partners in cyber security the Health Board is progressing at pace with finalising the recommendations of the Stratia Report and the work required to complete the Network and Information Systems Regulations (NISR) , which are due to be completed by December 2021. However, the remedial work undertaken as a result of the assessments is currently not funded and will provide a challenge to the Digital Team to deliver.

Network and Information Systems Regulations (NISR)

As mentioned within the report, the implementation of NISR will be a key directive for the Health Board in terms of Cyber Security. It is designed to protect critical national and local infrastructure against cyber-attacks. This regulation applies to all parts of the UK and European Union (EU) and came into force in May 2018, alongside the GDPR/Data Protection Act. As part of NHS Wales, HDdUHB is an Operator of Essential Services and has a legal obligation to comply with NISR and ensure that appropriate and proportionate security measures to manage risks to its network and information systems are undertaken. All cyber related incidents encountered by HDdUHB must be reported to the NHS Wales Cyber Resilience Unit (CRU) for onward reporting to Welsh Government (WG).

As part of the NIS Regulations, WG has been appointed as the Competent Authority and the National Cyber Security Centre (NCSC) has been appointed as the Computer Security Incident Response Team (CSIRT) and Single Point of Contact (SPOC). A Cyber Assessment Framework (CAF) has been developed by NCSC and a specific CAF has been tailored for NHS Wales by the NHS Wales CRU. The CAF will be used to assess current compliance against the regulations.

Corporate Risk 451

The corporate risk has been active since the WannaCry outbreak. However, it has been focussed on the impact of not having updated patching of desktops/laptops and server infrastructure. With the advent of the NIS Regulations, the risk will be reframed accordingly to provide a more general risk around Cyber Security, which incorporates the patching requirement in addition to compliance with the NIS Regulation. For instance, additional metrics will need to be developed to monitor the number of vulnerabilities within the Health Board, which can then be themed and risk assessed.

Next Steps

The proposed next steps to progress Cyber Security within the Health Board include:

- Establishing a Cyber Resilience Team, which builds on the current resources within the Digital Team. This team will work with the CRU and will also ensure that vulnerabilities are investigated and resolved, therefore strengthening cyber resilience
- Completion of the CAF to assess the compliance against the NIS regulations
- Following the completion of the assessment framework, development of an action plan with achievable timescales to be presented and monitored via the Information Governance Sub-Committee
- Closure of Risk 451 and development of a new risk, which details the wider implications of a lack of cyber resilience
- Development of a cyber resilience dashboard for scrutiny by the Information Governance Sub-Committee

Argymhelliad / Recommendation

The Sustainable Resources Committee is requested to note the contents of the report and support the next steps included within the report.

Amcanion: (rhaid cwblhau) **Objectives: (must be completed)**	
Committee ToR Reference: Cyfeirnod Cylch Gorchwyl y Pwyllgor:	3.10 Provide assurance to the Board that arrangements for information governance are robust.
Cyfeirnod Cofrestr Risg Datix a Sgôr Cyfredol: Datix Risk Register Reference and Score:	Risk Number 451 – Risk Score 12
Safon(au) Gofal ac Iechyd: Health and Care Standard(s):	3.4 Information Governance and Communications Technology 3.2 Communicating Effectively 4.2 Patient Information
Amcanion Strategol y BIP: UHB Strategic Objectives:	All Strategic Objectives are applicable
Amcanion Llesiant BIP: UHB Well-being Objectives: Hyperlink to HDdUHB Well-being Objectives Annual Report 2018-2019	10. Not Applicable

Gwybodaeth Ychwanegol: **Further Information:**	
Ar sail tystiolaeth: Evidence Base:	Not applicable
Rhestr Termau: Glossary of Terms:	Contained within the report
Partïon / Pwyllgorau â ymgynhorwyd ymlaen llaw y Pwyllgor Adnoddau Cynaliadwy: Parties / Committees consulted prior to Sustainable Resources Committee:	Information Governance Sub-Committee (IGSC)

Effaith: (rhaid cwblhau) **Impact: (must be completed)**	
Ariannol / Gwerth am Arian: **Financial / Service:**	Failure to meet Information Security will result in the Health Board not being fully compliant with information governance legislation and could result in significant fines. Failure to comply with the NIS regulations has the potential of a 2% of Revenue / Budget Fines for non-compliance or the potential to be fined 2% of Revenue / Budget under NISR and 4% / 2% of Revenue / Budget under GDPR 2018 in the event of a cyber security breach and resultant data theft / loss.
Ansawdd / Gofal Claf: **Quality / Patient Care:**	Failure to keep Person Identifiable information secure would be a breach of Data Protection Act and may result in a loss of patient confidence in the Health Board in relation to the safe keeping of data. Patient care could be impacted by outages caused by a successful Cyberbreach, as networks could be saturated, causing failure of diagnostic services and any ransomware attack could encrypt patient data so clinicians would not have the latest information available.
Gweithlu: **Workforce:**	Any Cyber breach would significantly impact the workforce as digital systems used to support day-to-day would potentially become unavailable.
Risg: **Risk:**	The Cyber Security risk is noted upon the Informatics Risk Register and also included within the Corporate Risk Register.
Cyfreithiol: **Legal:**	Failure to meet Information Security would result in the Health Board not being fully compliant with information governance legislation and could result in poor IG practices being in place throughout the Health Board. It may also lead to investigations by the Information Commissioner's Office, resulting in improvement demands or penalty notices.

Enw Da: **Reputational:**	The loss of data due to a cyber-attack would cause significant reputational damage to the Health Board.
Gyfrinachedd: **Privacy:**	Not Applicable
Cydraddoldeb: **Equality:**	Not Applicable