Bwrdd Iechyd Prifysgol Hywel Dda University Health Board

PWYLLGOR ADNODDAU CYNALIADWY
SUSTAINABLE RESOURCES COMMITTEE

DYDDIAD Y CYFARFOD: DATE OF MEETING:	25 April 2022
TEITL YR ADRODDIAD: TITLE OF REPORT:	Cyber Resilience and Security
CYFARWYDDWR ARWEINIOL: LEAD DIRECTOR:	Huw Thomas, Executive 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)

Ar Gyfer Trafodaeth/For Discussion

ADRODDIAD SCAA
SBAR REPORT

Sefyllfa / Situation

The purpose of this report is to provide the Sustainable Resources Committee with an update on the current heightened cyber security threat caused as a result of the conflict in Ukraine, and to provide a cyber-security update on vulnerabilities, alerts, incidents, and Security Architecture work.

Cefndir / Background

All NHS Wales organisations share a common Information and Communications Technology (ICT) network and many other common ICT systems such as the Microsoft Active Directory, Office 365, Welsh Laboratory Information Management System (WLIMS) and Welsh Clinical Portal (WCP). These various systems are inextricably linked and should essentially be regarded as a single shared ICT system. Consequently, every user in every organisation is required to take action to protect themselves and the wider NHS in Wales from a cyber-attack. Our networks and systems are very similar to those in the Health Service Executive (HSE) in Ireland, which was subject to a major cyber-attack in 2021, resulting in the disruption of ICT systems for around four months.

Following Russia's attack against Ukraine, there is a heightened cyber security threat for all organisations, with the National Cyber Security Centre (NCSC) calling on all UK organisations to bolster their cyber security defences. Therefore, the Hywel Dda University Health Board's (HDdUHB) Cyber Security team has been taking steps to improve the capability and resiliency to defend against and respond to a cyber-attack.

Asesiad / Assessment

CURRENT ADVICE
During the past month, there has been a heightened threat for a cyber security attack, with the NCSC calling for organisations to bolster their online defences. While the NCSC is **not** aware of any current specific threats to UK organisations in relation to events in and around Ukraine,

there has been a historical pattern of cyber-attacks against Ukraine with international consequences.

New malware and cyber tactics, techniques and procedures have been discovered recently, including new wiper malware, which erased data from systems to cause disruption. A new criminal group has been identified as LAPSUS$, which is known for data exfiltration and destruction. Successful attacks against NVIDIA, Samsung, Vodafone and UBISoft have already been attributed to this criminal group. There has also been a rise in 'hacktivism' since the attack on Ukraine, with recent Conti ransomware chats and details released to the public via the dark web. This has provided an insider view of how a ransomware group, which targeted the Ireland HSE, operates and highlights the real threat that our organisations face.

There are currently 45 known threat actors operating out of Russia with a total of 14 known to target the healthcare sector located in the United Kingdom. The most prolific threat actors include Wizard Spider (known to deploy Ransomware) and Cozy Spider, who are known to be state-sponsored and are utilising spear phishing campaigns to gain access to exfiltrate data and cause widespread disruption.

Although the NCSC is **not** aware of any current specific threats against NHS Wales and HDdUHB, the threat level has significantly increased.

HDdUHB's Cyber Security team is engaging with all NHS Wales organisations regarding this specific threat, and with National Local Authority Warning, Advice, and Reporting Point (NLAWARP) and the Dyfed Powys Local Resilience Forum (DPLRF).

Due to the heightened cyber security threat, the Cyber Security team is currently following NCSC guidance. The team is prepared to adapt to the situation if required. The team is making a concerted effort to identify threats that may be attributed to threat actors known to be operating out of Russia.

MITIGATIONS TAKEN

The Cyber Security team is rolling out Defender for Endpoint. New functionality has recently been added with the introduction of the Microsoft E5 licence, providing visibility of user cloud sign-in and on-premise user behaviour.

To complement the new functionality of Defender for Endpoint, Microsoft Cloud App Security (MCAS) and Microsoft Identity, the Cyber Security team has also introduced an automated malware analysis tool and cyber threat intelligence with a focus on healthcare. These new tools provide the threat intelligence required to speed up an incident response.

The Cyber Security team continues to provide security architecture advice, ensuring designs follow security best practice and follow the requirements of the Network and Information Systems Regulations (NIS-R). The team has also made progress with the tools and capabilities available to HDdUHB. These capabilities have had a positive impact on the requirements to bolster cyber defence and include:

- Onboarding HDdUHB to the NCSC early warning system
- Ingestion of focused health and pharmaceutical threat feeds into Splunk, which is the software for monitoring, and analysing machine generated data to identify any themes that could be classified as a malicious action
- Additional servers have been onboarded to the vulnerability management service
- Piloting of Microsoft Managed Desktop
- Introduction of a new patch testing group to speed up the patching process

- Introduction of HDdUHB managed remote control solution to assist with third party vendor access
- Automated monitoring of HDdUHB assigned public Internet Protocol (IP) addresses
- Releasing updated guidance to staff relating to phishing emails, unusual activity of desktops via unexpected pop-ups, re-enforcing password advice, and ensuring that all desktops / laptops are security patched
- The Digital Team convene a weekly technical meeting to discuss the cyber threat to the Health Board and agree any specific actions required to react to the current threat status
- A robust Cyber Programme is in development to ensure that the Health Board becomes compliant with the NIS-R.

SUMMARY

In summary:

- Considering the heightened cyber security threat, the Cyber Security team continues to increase cyber defences at pace.
- The NCSC is **not** aware of any current specific threats against NHS Wales and HDdUHB as a result of the events in and around Ukraine. However, the threat level has significantly increased.
- It is also recommended that departments should test their business continuity plans in regard to a possible cyber-attack and any requirement to switch-off the ICT infrastructure

Argymhelliad / Recommendation

The Sustainable Resources Committee is requested to:

- **NOTE** the contents of this report, and the fact that NCSC is **not** aware of any current specific threats against NHS Wales and HDdUHB.
- **NOTE** the heightened security currently within NHS Wales and the ongoing work that the Cyber Security team is undertaking locally.
- **RECOMMEND** that departments formally test their business continuity plans in regard to a possible cyber-attack.

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 1352 – Risk Score 16
Safon(au) Gofal ac Iechyd: Health and Care Standard(s):	3.4 Information Governance and Communications Technology
Amcanion Strategol y BIP: UHB Strategic Objectives:	Not 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:	NISR Cyber Assessment Framework Interviews with Health Board Staff
Rhestr Termau: Glossary of Terms:	Included within the body of 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) Executive Team

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-Rhas the potential of a 2% of Revenue / Budget Fines for noncompliance or the potential to be fined 2% (up to £17m) of Revenue / Budget under NISR and 4% / 2% of Revenue / Budget under General Data Protection Regulations (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 patient monitoring, non-availability of patient data and/ or a clinical accident due to tampering of patient data.
Gweithlu: Workforce:	Any Cyber breach would significantly impact the workforce as digital systems used to support day-to-day would potentially become unavailable. These include staff rostering, pay, procurement, security swipes, in addition to networked clinical systems, air handlers, laboratories etc.
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 Information Governance (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 and risk of individual litigation cases.
Gyfrinachedd: **Privacy:**	Any Cyber Security breach that results in Data Theft will have an impact on both patients and staff privacy.
Cydraddoldeb: **Equality:**	Not Applicable