Bwrdd Iechyd Prifysgol Bae Abertawe
Swansea Bay University Health Board

Cadeirydd/Chair: **Emma Woollett**
Prif Weithredwr/Chief Executive: **Mark Hackett**

gofalu am ein gilydd, cydweithio, gwella bob amser
caring for each other, working together, always improving

Cais Rhyddid Gwybodaeth / Freedom of Information request
Ein Cyf / Our Ref: 23-A-034

You asked:

1. **What was the total number of cyber attack incidents that have been recorded in your Health Board in the past 24 months?**
   Three incidents

2. **What is the classification of your policy regarding breach response?**
   A cyber breach is reported to the Cyber Resilience Unit in Digital Health & Care Wales (DHCW), and also potentially via the Information Commissioners Office (ICO) if Data Protection has also been impacted.

3. **Of the devices running Windows operating systems, what is the number and percentage of devices running Windows 11, Windows 10, Windows 7, Windows XP?**
   I can confirm that the Health Board holds this information. However, this is withheld under Section 31(1)(a). See below for details.

4. **What are the top 20 cyber security risks in your Health Board, and how are they managed?**
   I can confirm that the Health Board holds this information. However, this is withheld under Section 31(1)(a). See below for details.

5. **Do you continue to use the Unified Cyber Risk Framework, is so how many risks are still identified/managed.**
   No

6. **What is your Patch Management Cycle and how is it implemented on old Operating systems (e.g., for Windows , Windows XP)?**
   I can confirm that the Health Board holds this information. However, this is withheld under Section 31(1)(a). See below for details.

7. **What is your current status on unpatched Operating Systems?**

I can confirm that the Health Board holds this information. However, this is withheld under Section 31(1)(a). See below for details.

8. **Of the devices running Windows Servers operating systems, what is the number and percentage of devices running Windows 2000, Windows 2003, Windows 2008, Windows 2012, Windows 2016, Windows 2019, Windows 2022?**
   I can confirm that the Health Board holds this information. However, this is withheld under Section 31(1)(a). See below for details.

9. **Has your Health Board signed up to and implemented the NHS Secure Boundary managed service to strengthen cyber resilience? If so, how many cyber security threats has the NHS Secure Boundary detected within your NHS Trust since its implementation?**
   No, this is only relevant in NHS England

10. **Does your Health Board hold a cyber insurance policy? If so:**

    a. What is the name of the provider;

    b. How much does the service cost; and

    c. By how much has the price of the service increased year-to-year over the last three years?

    I can confirm that the Health Board does not hold a cyber insurance policy.

11. **When did the current Board last receive a briefing on cybersecurity threats within healthcare, and when did they last participate in cyber security training? How frequently, if at all, do these briefings and trainings occur, and are they carried out by cyber security technology professionals?**
    Board members are sent cyber awareness information on a monthly basis, as do all staff. The Board also received a Cyber development session in October 2021 highlighting cyber risks and awareness on the NCSC Board toolkit.

12. **Has your Health Board completed a Connection Agreement to use the Health and Social Care Network (HSCN)? If so, did you pass, and is there a copy of the code of connection?**
    NHS Wales has HSCN. I can confirm that the Health Board uses the NHS Wales HSCN connection.

13. **Have there been any incidents of staff members or personnel within your Health Board being let go due to issues surrounding cyber security governance?**
    No

14. **How many open vacancies for cyber security positions are there within your Health Board, and is their hour capacity affected by a shortage of qualified applicants?**
    One vacancy, not known, as in process of going to recruitment.

15. **Are there mandatory minimum training requirements for those transferred internally to work in cybersecurity within your Health Board, and if so, how often is the training updated and revised to reflect the evolving nature of the industry?**
    Each job role will have essential and desired qualifications.

16. **How much money is spent by your Health Board per year on public relations related to cyber attacks? What percentage of your overall budget does this amount to?**
    The Health Board does not have a dedicated budget.

17. **Does your Health Board have a Chief Information Risk Officer? If so, who do they report to?**
    No, the Health Board has a SIRO (Senior Information Risk Owner) that leads on risk within the Health Board and reports to the Health Boards CEO.

18. **When was the last time your Health Board underwent a security audit? At what frequency do these audits occur?**
    November 2022, these audits are conducted annually.

19. **What is your strategy to ensure security in cloud computing?**
    Under Development as SBU building a Cloud Computing business case. Software as a service e.g. Office 365 and other applications have robust security certifications and assessments in place

20. **Do you purchase additional / enhanced support from a Supplier for end-of-life software (Operating Systems / Applications)? If so, what are the associated costs per year per Operating System / Application, and the total spend for enhanced support?**
    I can confirm that the Health Board holds this information. However, this is withheld under Section 31(1)(a). See below for details.

<u>For Questions 3, 4, 6, 7 and 20 the following FOIA exemption applies:</u>

I can confirm that the Health Board holds this information. However, disclosure of information on the internet capable hardware, software and operating systems used by the Health Board would constitute a security risk by leaving the health boards networked computer systems more vulnerable to a malicious attack.

Section 31(1)(a) states that information is exempt if its disclosure is likely to prejudice the prevention or detection of crime. ICO guidance states that this can be used to protect information on a public authority's systems which would make it more vulnerable to crime. It can be used by a public authority that has no law enforcement function:

- To protect the work of one that does.
- To withhold information that would make anyone, including the public authority itself, more vulnerable to crime.

The crime in question here would be a malicious attack on the health boards computer systems. Since the disclosure of the withheld information would make the health

boards systems more vulnerable to much crime this review finds that the exemption is engaged.

The exemption is subject to the public interest test. There is an overwhelming public interest in keeping Health Board systems secure which would be served by non-disclosure. This outweighs the public interest in accountability and transparent which would be served by disclosure.
