Reference:	FOI.10697.23
Subject:	Cyber security and attacks
Date of Request:	16 January 2023

Requested:

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

2. What is the classification of your policy regarding breach response?

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?

4. What are the top 20 cyber security risks in your Trust, and how are they managed?

5. Do you continue to use the Unified Cyber Risk Framework, is so how many risks are still identified/managed.

6. What is your Patch Management Cycle and how is it implemented on old Operating systems (e.g., for Windows , Windows XP)?

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

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?

9. Has your Trust 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?

10. Does your Trust 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?

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?

12. Has your NHS Trust 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?

13. Have there been any incidents of staff members or personnel within your Trust being let go due to issues surrounding cyber security governance?

14. How many open vacancies for cyber security positions are there within your Trust, and is their hour capacity affected by a shortage of qualified applicants?

15. Are there mandatory minimum training requirements for those transferred internally to work in cybersecurity within your Trust, and if so, how often is the training updated and revised to reflect the evolving nature of the industry?

16. How much money is spent by your Trust per year on public relations related to cyber attacks? What percentage of your overall budget does this amount to?

17. Does your Trust have a Chief Information Risk Officer? If so, who do they report to?

18. When was the last time your Trust underwent a security audit? At what frequency do these audits occur?

19. What is your strategy to ensure security in cloud computing?

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?

Response:

Hywel Dda University Health Board (UHB) is unable to provide all of the information requested, as it has deemed that the information is exempt from disclosure under Section 31(1)(a) of the Freedom of Information Act 2000 (FoIA). The UHB has also considered the "mosaic effect"; the harm which will or will be likely to arise from the release of this information, along with information already in the public domain.

Section 31(1)(a) of the FoIA provides that information which is not exempt by virtue of Section 30 (criminal investigations and proceedings) is exempt if its disclosure would, or would be likely to, prejudice the prevention or detection of crime. The Information Commissioner's Office (ICO) guidance advises that Section 31, amongst other things, prevents information being disclosed that would increase the risk of the law being broken. In addition, it can be claimed by any public authority. The UHB is relying upon this exemption as it considers that releasing this information for questions 3, 4, 6, 7, 8, 9 and 20 relating to our IT systems, would in the present climate, make it more vulnerable to crime.

Section 31(3) of the FoIA provides that the duty to confirm or deny does not arise in relation to this information.

Section 31 of the FoIA is subject to the public interest test.

In favour of disclosure: The UHB has a duty to maintain openness and transparency in all its activities, which will help to maintain public trust in the UHB.

In favour of non-disclosure: By releasing the information, the UHB would be vulnerable to this being used for crime, which potentially could compromise the security of both patient and staff information, whilst causing disruption to the flow of information through the UHB systems, impacting on patient care and safety. There is a clear public interest in protecting society and the UHB from the impact of crime. The UHB has given consideration to a cyber-attack in the NHS, in recent years, which is already in the public domain.

Decision: The UHB considers that the public interest in withholding the information for questions 3, 4, 6, 7, 8, 9 and 20 is greater than the interest in disclosing, therefore protecting the UHB from potential criminal activity.

However, the UHB provides responses to the other requests below.

1. The UHB confirms that fourteen (14) cyber-attack incidents were recorded during the past twenty-four (24) months.

2. The UHB confirms that for breach responses, it follows the National Cyber Security Centre (NCSC) guidance to classify the severity.

3. & 4. Section 31 exemption applied.

5. The UHB confirms that all risks are manged using its risk framework, which is available on our website. For ease, the link has been provided below:

   https://hduhb.nhs.wales/about-us/governance-arrangements/policies-and-written-control-documents/policies/risk-management-framework/

   Additionally, the UHB currently has ten (10) cyber security risks identified.

6. to 9. Section 31 exemption applied.

10. The UHB confirms that its cyber insurance is provided on an All Wales basis via NHS Wales Shared Partnership (NWSSP) Legal and Risk Service and covers all potential insurance liabilities. Further information can be found on the NWSSP Welsh Risk Pool website. For ease, the link has been provided below:

    Welsh Risk Pool - NHS Wales Shared Services Partnership

    There are no specific costs associated with cyber insurance policies.

11. The UHB confirms that its last briefing and training on cyber security threats within healthcare, was in October 2022. Training is provided annually by a professional cyber security training organisation.

12. The UHB does not hold the information requested, as it is managed by Digital Health and Care Wales (DHCW). Therefore, please re-direct this part of your request to its Freedom of Information (FoI) Team, who may be able to help you with your enquiry. Contact details are as follows:-

    DHCW.FOI@wales.nhs.uk or alternatively, you can contact: Freedom of Information Team, Digital Health and Care Wales, Ty Glan-yr-Afon, 21 Cowbridge Road East, Cardiff, CF11 9AD.

13. The UHB confirms that there have been no incidents of staff members being terminated due to issues surrounding cyber security governance.

14. The UHB confirms that it currently has one (1) open vacancy for a cyber security position. However, the UHB does not hold the information on the suitability, as the position is still being advertised.

15. The UHB confirms that there are no mandatory minimum training requirements in place for internal staff transferring into cyber security.

16. The UHB confirms that it has not spent any money on public relations relating to cyber attacks.

17. The UHB does not have a Chief Information Risk Officer. However, the UHB's Senior Information Risk Owner is Executive Director Huw Thomas, Director of Finance.

18. The UHB confirms that the last security audit was undertaken in October 2022, and it endeavours to undertake these audits on an annual basis.

19. The UHB confirms that its strategy in ensuring security in cloud computing is aligned to the National Cyber Security Centre's (NCSC) Cyber Security Centre Cloud Security. For ease of reference, the link to the guidance has been provided below:

    Cloud security guidance - NCSC.GOV.UK

20. Section 31 exemption applied.