Freedom of Information Request: Our Reference CTMUHB_29_23

You asked:

I am writing to you to request the following information about your NHS Trust under section 1(1) of the Freedom of Information Act 2000:

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

   Due to the scale of our organisation, we are subject to many cyber events. However, there have been no successful cyber attacks on locally hosted systems during the period requested.

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

   This question requires further clarification. However, we have agreed to adopt the NIST Cybersecurity framework and to the ongoing dynamic improvement of our incident response plan. This plan is frequently tested & improved.

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?**

   In accordance with the Freedom of Information Act 2000, this acts as a Refusal Notice under section 17 of the Act.

   Cwm Taf Morgannwg University Health Board has deemed that the information requested is exempt from disclosure under Section 31(1)(a) and Section 38(1)(a)&(b) of the Freedom of Information Act 2000 (the Act).

   The University Health Board (UHB) recognises its duty to protect the public and individuals, and we will not jeopardise this duty by providing this information. In our opinion, this would weaken our ability to protect our patients, staff and other service users. We have also considered 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 Act 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. In guidance, the Information Commissioner's Office has advised 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.

   Revealing system details into the public domain would make this information accessible to criminals and cyber terrorists and subsequently compromise public and individual safety.

Section 38(1)(b) – endanger the safety of any individual. Providing this information could enable hackers and cyber criminals to gain knowledge about the Health Boards capabilities and IT security measures, and this could enable them to plan attacks where they perceive a lower level of security resource exists. This exposes our IT systems to greater risk and therefore, constitutes a risk to both public and staff, as our systems are used to provide patient care.

The UHB is relying upon these exemptions as it considers that releasing this information about our IT systems, would in the present climate, make it more vulnerable to crime.

Section 31 – Law Enforcement of the Act states that:

31(1) Information which is not exempt information by virtue of section 30 is exempt information if its disclosure under this Act would, or would be likely to, prejudice - (a) the prevention or detection of crime

Section 38 – Health and Safety of the Act – states that:

38(1) Information is exempt information if its disclosure under this Act would, or would be likely to –
(a) endanger the physical or mental health of any individual, or
(b) endanger the safety of any individual.
(2) The duty to confirm or deny does not arise if, or to the extent that, compliance with section 1(1)(a) would, or would be likely to, have either of the effects mentioned in subsection (1).

Therefore, the UHB considers that the public interest in withholding the information outweighs any arguments for disclosure, therefore protecting the Health Board from potential criminal activity.

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

Our risks are communicated to board via the relevant committee, these are not for public disclosure (Please see response to question 3). They are managed through an integrated Cyber Improvement Plan and are externally monitored by the NHS Wales Cyber Resilience Unit.

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

Risks are identified and managed through Corporate risk management approaches. This also incorporates NIS-D risks and other related to Cyber based on frameworks including NIST.

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

Please see response to question3.

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

   Please see response to question 3.

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?**

   Please see response to question 3.

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?**

   Please see response to question 3.

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?**

    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. Please see link provided below:

    Welsh Risk Pool.

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?**

    Briefings are provided quarterly. A training and awareness session was carried out in the past 3 months, delivered by a combination of victims, the police and the Cyber team within the University Health Board (UHB).

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?**

    This is managed by Digital Health and Care Wales (DHCW). For further information, please contact DHCW directly.

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

If let go means dismissed, or not having their contract renewed, the answer is yes.

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?**

    There are 2 vacancies currently being authorised/advertised.

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?**

    All ICT staff will consume internally published Cyber Training and will receive at the desk training by line managers. Senior members of the team are required to have attended the NIST Cybersecurity practitioner course.

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?**

    None.

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

    No. We have a Senior Information Risk Officer. They report to the Chief Executive.

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

    Within the last 3 months. There are multiple audits carried out per year.

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

    Cloud Security Assessment as part of Cyber Security Assessment for any new service.

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?**

    Please see response to question 3.