Maidstone and Tunbridge Wells NHS Trust

Ref: FOI/GS/ID 7942

Please reply to:
FOI Administrator
Trust Management
Maidstone Hospital
Hermitage Lane
Maidstone, Kent
ME16 9QQ
Email: mtw-tr.foiadmin@nhs.net
www.mtw.nhs.uk

10 May 2023

Freedom of Information Act 2000

I am writing in response to your request for information made under the Freedom of Information Act 2000 in relation to Cyber security.

You asked: All questions are shown as received by the Trust.
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?

Trust response:
1. Zero
11. The Board receive a quarterly report on cyber security threats applicable to our sector. They received training in November 2022 and this will be renewed annually.
14. None
15. Yes with the requirements being continually reviewed and updated when applicable.
17. The Trust SIRO is the 'Director of Strategy, Planning and Partnerships' who reports to the Chief Executive Officer and also the Trust Board.

The trust has applied Section 31 (1)(a) of the FOI Act (Law Enforcement) to the remaining questions as providing this information could compromise the security of the Trust's network / data and might materially cover activity which forms part of ongoing criminal investigations

The information which has been withheld is exempt from disclosure under section 31(1)(a) of the Freedom of Information Act. The relevant parts of the ICO guidance on the subject (https://ico.org.uk/media/for-organisations/documents/1207/law-enforcement-foi-section-31.pdf) run as follows:

31.(1) Information is exempt if its disclosure under this Act would, or would be likely to, prejudice - (a) the prevention or detection of crime. It could be used to withhold information that would make anyone, including the public authority itself, more vulnerable to crime for example, by disclosing its own security procedures. It is the view of this trust's Information security function that disclosure of the information above would prejudice our ability to resist cyber-attacks, etc. on our systems.

The Trust has a dedicated Cyber Security team and has purchased and installed many different solutions to help protect us against cyber threats. However, we will not be publicising or sharing the details of these products, solutions or vendors because we believe that in doing so, we put our self at risk.

We will also not be publishing details around any system be it hardware or software that is either end of life or is coming to end of life as we believe that publishing this information also puts the trust at risk. This would include but is not limited to items such as "does the trust have any machines running an out of date operating system or unsupported hardware".