Request for information under the Freedom of Information Act – 2023.304
Released – 9 February 2023

Thank you for your email received 16 January 2023 requesting information regarding cyber security.

Please find detailed below a summary of your request, together with our response.

Summary of your original request:
1. What was the total number of cyber attack incidents that have been recorded in your trust in the past 24 months?
No cyber attack incidents recorded in last 24 months.

2. What is the classification of your policy regarding breach response?
The Data Security and Protection policy version 1.7 is live and available on our public website here: https://www.kentcht.nhs.uk/about-us/our-aims/our-policies-and-procedures/ The policy is due to undergo some minor alterations to update some of the job titles and will be re-published on our public website and internal intranet site in the near future. Incident and risk management is cover under section 17 of the policy. Incidents must be reported immediately and no longer than 24 hours after the event.

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?
5872, all Windows 10

4. What are the top 20 cyber security risks in your Trust, and how are they managed?
We do not have categorised Cyber Security Risks in order. We manage risk through implementation of Process, Policy and Procedure.

5. Do you continue to use the Unified Cyber Risk Framework, is so how many risks are still identified/managed.
We do not use the Unified Cyber Risk Framework

6. What is your Patch Management Cycle and how is it implemented on old Operating systems (e.g., for Windows , Windows XP)?
We install patches within 14 days of release. Patch management is delivered via Ivanti (EUC devices) and WSUS (server and infrastructure environment). This includes old operating systems, if we were to have any.

7. What is your current status on unpatched Operating Systems?
Unpatched operating systems will be captured within the patch ring process and deployed within 14 days of release. If a device falls outside of this timeframe (due to being uncontactable for any reason) then it will be captured as soon as it appears online.

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?
125 virtual machines, 6 running Server 2012 and 119 running Server 2019

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?
Yes, we use NHSD Secure Boundary. Threat detection for last 90 days is 30,900 blocked events.

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?
The Trust is not able to confirm or deny if it holds any relevant information in response to this part of your request under Section 38(2) Health and Safety of the Freedom of Information Act 2000. We feel that if we were to confirm or deny if we held this information it could endanger the safety of individuals as it may leave the Trust vulnerable to cyber attacks. I have detailed below the relevant excerpt from the Act:

> ***Section 38 – Health and safety***
>
> *(1) Information is exempt information if its disclosure under this Act would, or would be likely to -*
>
> *(a) endanger the physical or mental health or 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 within subsection (1).*

<u>Prejudice</u>
Confirming or denying that we hold the information requested would prejudice the health and safety of the Trust's buildings, patients, staff and members of the public.

Section 38 is a prejudice-based exemption and subject to a public interest test. This means that not only does the information have to prejudice one of the purposes listed, but before the information can be withheld, the public interest in preventing that prejudice must outweigh the public interest in disclosure.

Public Interest Test

Considerations in favour of disclosure:

- The inherent public interest in the openness and transparency of public authority dealings
- The public have a right to know whether authorities have robust security measures in place

Considerations against disclosure:

- The requested information is a control measure to protect Trust systems; if the Trust were to confirm or deny if it held the information requested and this was to be released into the public domain it would reveal our position, weaken our cyber security posture and could increase our risk of attack
- Disclosing this information would increase the vulnerability of specific NHS organisations on a national level leading to the disruption of NHS organisations' ability to conduct business
- Applying this exemption will prevent the disclosure of information that could endanger the safety of individuals
- A successful attack would have a direct impact on the health and safety of patients

Conclusion:

The Trust recognises that there is a public interest in the disclosure of information which facilitates the accountability and transparency of public bodies for decisions taken by them and would demonstrate that the Trust has robust security measures in place. However, there is also a public interest in the security of the Trust's buildings, staff, patients and visitors which is put to the wider public interest.

Having undertaken the balancing exercise, the Trust has concluded that the public interest in maintaining the exemption significantly outweighs the public interest in confirming or denying if we hold any relevant information. Particular weight has been placed on the severity of the prejudice which may be caused were the Trust to release the requested information.

Given that the definition of 'public' under the Act is considered to be the public at large, rather than just the individual applicant or a small group of people and that 'public interest' is not necessarily the same as what interests the public, it is considered that confirming or denying if we hold this information is likely to result in prejudice to the health and safety of the Trust's patients, which is not outweighed by the wider public interest for disclosure.

The Trust considers that the greater public interest lies with protecting staff, patients, and general members of the public which means disclosure cannot be justified.

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?

The board receive a cyber security briefing every 6 months. Each Board member completes an online data security and protection training module provided by Health Education England through their e-Learning for Healthcare portal. The renewal date will vary for each Board

member, depending on when they started working for the organisation. In March 2022 the Board received NHS Digital's National Cyber Security Centre (NCSC) certified board-level training which was delivered by their training partner Templar Executives. The Board are scheduled to receive further board-level data protection and cyber-security training in March 2023 which will be delivered by an external data protection compliance consultant and training provider.

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?
Yes, this was completed and managed on our behalf by our HSCN provider; therefore we are not able to provide 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?
No.

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?
1 vacancy currently open. Yes, capacity to fulfil the vacancy is affected by availability of 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?
Someone transferring internally would be required to fill the job specification before being offered the role. We currently have one vacancy within this area so the training would have been updated and revised prior to this post being advertised.

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?
There have been no cyber attacks in the past 12 months and no money has been spent on public relations relating to cyber attacks at the trust. If a cyber attack were to take place, the communications around this would be managed by our in-house Communications Team.

17. Does your Trust have a Chief Information Risk Officer? If so, who do they report to?
We have a SIRO (Senior Information Risk Officer), and they report directly to the Chief Executive.

18. When was the last time your Trust underwent a security audit? At what frequency do these audits occur?
We offer compliance returns annually in the form of DSPT

19. What is your strategy to ensure security in cloud computing?
We are not engaged in Cloud computing currently

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?
Not applicable from an endpoint or server operating system perspective.