The Tavistock and Portman
NHS Foundation Trust

Freedom of Information Act 2000 disclosure log entry

Reference

Date response sent

Subject

Details of enquiry

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 sent

Your request received 19 January 2023 and has been handled under the Freedom of Information Act (FOIA). Please see below our response.

FOIA applies to existing recorded information and does not require the authority to answer questions or otherwise respond where this would involve the creation of new information.

Some of your 20 questions would involve creation of new information, where data requested is not held in any defined document(s) or database(s) or in a way that is sufficiently structured to enable the data to be located and extracted.

Please note that, as required under the ICO model publication scheme;

a) the Trust publishes all monthly expenditure that exceeds £25,000 at https://tavistockandportman.nhs.uk/about.us/governance/trust-expenditure-over-25000/ where you may find that some spend data which you seek, is already published
b) The Trust publishes most of the substantive responses to FOI requests on its website, within a dedicated Disclosure Log section FoI disclosure log (tavistockandportman.nhs.uk).

1. What was the total number of cyber attack incidents that have been recorded in your trust in the past 24 months?
   Withheld under s31a of the Freedom of Information Act 2000 (FOIA)
2. What is the classification of your policy regarding breach response?
   We do not classify our policies. They are all publicly available on our website.
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?
   All our endpoint devices are running on Windows 10
4. What are the top 20 cyber security risks in your Trust, and how are they managed?
   Withheld under s31a of the Freedom of Information Act 2000 (FOIA)
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)?
   We have a monthly and ad hoc patch routine. We are up to date with our patch management
7. What is your current status on unpatched Operating Systems?

Not applicable. See response to Q 6 above

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?
   Data withheld under s31a of the Freedom of Information Act 2000 (FOIA)
9. Has your Trust signed up to and implemented the NHS Secure Boundary managed service to strengthen cyber resilience?
   Yes

   If so, how many cyber security threats has the NHS Secure Boundary detected within your NHS Trust since its implementation?
   Data withheld under s31a of the Freedom of Information Act 2000 (FOIA)
10. Does your Trust hold a cyber insurance policy? If so:
    No
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 received cyber security training, on 29th June 2021.
    - The Board received briefings on cyber security at the Board meeting on 27th September 2022.
    - Annually
    - These are carried out by external cyber security technology professionals.
12. Has your NHS Trust completed a Connection Agreement to use the Health and Social Care Network (HSCN)?
    Yes

    If so, did you pass, and is there a copy of the code of connection?
    Yes The Trust did pass and Yes there is 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?
    We confirm that there have been no instances of employees being dismissed due to issues surrounding cyber security governance within the last 5 years.
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?

    Nil vacancies for cyber security positions. All our vacancies are posted on our website at Current vacancies (tavistockandportman.nhs.uk) which includes job details and requirements.

    We so not hold data capacities affected by any staff or applicant shortages and this would involve the creation of new data, which – as explained above – is not required under FOIA.
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 our vacancies are advertised internally and then externally, which include provision of full job description and person specification. Please refer to our response to Q 14 above.
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?

We do not have a specific budget for communications around cyber attacks, and are therefore unable to answer this question

17. Does your Trust have a Chief Information Risk Officer? If so, who do they report to?
    The Trust has a SIRO (Senior Information Risk Officer) who reports to the Chief Executive
18. When was the last time your Trust underwent a security audit? At what frequency do these audits occur?
    In April 2022. These are carried out annually.
19. What is your strategy to ensure security in cloud computing?
    The Trust does not have an approved strategy for secure 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?
    No

With regards to the exemption engaged under s.31(a) of the FOIA, *Law Enforcement: the prevention or detection* of crime, this is a qualified exemption that requires the authority to carry out the public interest test. We have carried out the public interest test and have set out below the public interest arguments which we have considered:

Arguments in favour of disclosure:

- Promoting accountability and transparency on how public funds are utilised and spent

Arguments in favour of maintaining the exemption:

- The Trust has a duty to ensure that its information systems and assets are kept secure
- Disclosure of the requested information could facilitate criminal activity, in particular cybercrime, and especially when combined with other information already in the public domain or which could be gleaned from other sources, including any information that the Trust has previously provided or may be forced to disclose in the future.
- Disclosure of the requested information could, therefore, increase vulnerability to malicious attack, including the corruption or loss of data, software, hardware or other equipment, which would impact on the Trust's ability to provide essential services
- These vulnerabilities could extend to suppliers on whose services the Trust relies.

We have concluded that, on balance, the public interest in maintaining the exemption outweighs the public interest in disclosure.

We hope that you are satisfied with this response. If you are dissatisfied you can ask us to carry out an internal review of our handling of your request. You can request a review by emailing us at FOI@tavi-port.nhs.uk. Your review will be carried out by a senior officer within the Trust. If you remain dissatisfied following completion of our internal review, you have a right to complain to the Information Commissioner's Office (ICO) at https://ico.org.uk/make-a-complaint/official-information-concerns-report/official-information-concern/ or visit https://ico.org.uk/global/privacy-notice/how-you-can-contact-us/.