FOI_1028_2022-23 – FOI Request Concerning – Cyber Incidents

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

   No cyber-attacks have impacted the Trust in the past 24 months

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

   Confidential

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?**

   Please note, providing a response to this question, if applicable, could leave the Trust vulnerable to a cyber security attack and therefore the Trust has determined that he cannot provide a response to this request, for security reasons.

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

   The top 20 cyber security risks can not be shared, as they could leave the Trust vulnerable to a cyber security attack.

   We can advise that the cyber security risks are managed and monitored through the Information & Cyber Security Group and a Senior Information Risk Owner Meeting, both of which are held monthly.

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

   Yes

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

   Please note, providing a response to this question, if applicable, could leave the Trust vulnerable to a cyber security attack and therefore the Trust has determined that he cannot provide a response to this request, for security reasons.

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

   Please note, providing a response to this question, if applicable, could leave the Trust vulnerable to a cyber security attack and therefore the Trust has determined that he cannot provide a response to this request, for security reasons.

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 note, providing a response to this question, if applicable, could leave the Trust vulnerable to a cyber security attack and therefore the Trust has determined that he cannot provide a response to this request, for security reasons.

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

10. **Does your Trust hold a cyber insurance policy?**

    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 last received a cyber briefing in October 2022.

    The Board last received Board level cyber training July 2021. The Board, as with all staff within the Trust, do receive annual cyber training. Additionally, Board level cyber training is currently in the process of being arranged.

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?**

    No

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?**

    Currently have one Cyber Security Manager post vacancy. The second part of this question is unknown at present.

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?**

    N/A at present

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?**

    N/A

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

    The Trust has a Senior Information Risk Owner, who is Board Level and reports to the Trust's CEO.

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

    July 2021. A penetration test is undertaken annually.

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

    Please note, providing a response to this question, if applicable, could leave the Trust vulnerable to a cyber security attack and therefore the Trust has determined that he cannot provide a response to this request, for security reasons.

19. **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 note, providing a response to this question, if applicable, could leave the Trust vulnerable to a cyber security attack and therefore the Trust has determined that he cannot provide a response to this request, for security reasons.