Royal Devon University Healthcare NHS Foundation Trust

Title:

Cyber Security/Network Tracking

Reference Number: RDF100X
Date of Response: 18/04/2023

Further to your Freedom of Information Act request, please find the Trust's response(s) below:

1. *What is your primary inventory method for tracking each device type connected to the network?*
   - *IT devices (i.e. pc, laptop)*
   - *CMDB*
   - *Manual spreadsheet*
   - *Automated device detection*
   - *Other*
   - *None*

2. *IoT (i.e smart Tvs, smart watches,, assistants like Alexa, Siri)*
   - *CMDB*
   - *Manual spreadsheet*
   - *Automated device detection*
   - *Other*
   - *None*

3. *OT and building automation*
   - *(i.e. heating and cooling, routers, switches)*
   - *CMDB*
   - *Manual spreadsheet*
   - *Automated device detection*
   - *Other*
   - *None*

4. *Approximately how long does it take for the Trust to assess on Data Security and Protection Toolkit (DSPT)? What takes the most time?*
   Annual changes to DSPT take time for organisations to adjust, the scale of these changes varies from minor clarifications to new requirements and as such the amount of time varies accordingly. Some changes could take a year to implement if funding is required.

Section 31 (3) – Cyber Security

The Trust cannot provide the requested information for the remaining questions (questions ,6,7,8,9,10,11,12,13,14,15,16,17,18,19,and 20 below) under Section 31(3) of the FOIA.

Section 31(3) of the Freedom of Information Act allows a public authority to neither confirm nor deny whether it holds information where such confirmation would be likely to prejudice any of the matters outlined in section 31(1). This

includes information the disclosure of which would or would be likely to prejudice the prevention or detection of crime. Section 31(3) is subject to a public interest test for determining whether the public interest lies in confirming if the information is held or not.

Factors in favour of confirming or denying the information is held.

The Trust considers that to release the requested information would reveal details that could assist in a cyber-attack. However the Trust recognises that answering the request would promote openness and transparency with regards to the Trust's IT security.

Cyber-attacks which may amount to criminal offences under the Computer Misuse Act 1990 or the Data Protection Act 2018, are rated as a Tier 1 threat by the UK Government. The Trust like any organisation may be subject to cyber-attacks and since it holds large amounts of sensitive, personal, and confidential information, maintaining the security of this information is extremely important.

In this context, the Trust considers that providing the requested information would also provide information about the Trust's information systems and its resilience to cyber-attacks. There is a very strong public interest in preventing the Trust's information systems from being subject to cyber-attacks. Releasing the type of information requested would be likely to prejudice the prevention of cybercrime, and this is not in the public interest.

As an Operator of Essential Services: (https://www.legislation.gov.uk/uksi/2018/506/schedule/2/paragraph/8), the Trust must comply with The Network and Information Systems Regulations 2018. By releasing information that could increase the likelihood or severity of a cyber-attack, the Trust would fail to meet its security duties as stated in section 10 (https://www.legislation.gov.uk/uksi/2018/506/regulation/10) of the Network and Information Systems Regulations 2018.

The prejudice in complying with Section 31(3) of FOIA is real and significant and would allow valuable insight into the perceived strengths and weaknesses of the Trust's IT infrastructure and information systems.

5. *Connected Medical devices / IoMT (i.e. remote health monitoring devices, robotic surgery, imaging machines, MRI scanner)*

- *CMDB*
- *Manual spreadsheet*
- *Automated device detection*
- *Other*
- *None*

6. *How often is the information on those systems updated?*

- *IT devices (i.e. pc, laptop)*
- *As changes occur (real-time)*
- *Daily*
- *Weekly*
- *Monthly*
- *Quarterly*

- *Annually*
- *Never*
- *I don't know*

7. *IoT (i.e smart Tvs, smart watches,, assistants like Alexa, Siri)*
As changes occur (real-time)
- *Daily*
- *Weekly*
- *Monthly*
- *Quarterly*
- *Annually*
- *Never*
- *I don't know*

8. *Connected Medical devices / IoMT (i.e. remote health monitoring devices, robotic surgery, imaging machines, MRI scanner)*
As changes occur (real-time)
- *Daily*
- *Weekly*
- *Monthly*
- *Quarterly*
- *Annually*
- *Never*
- *I don't know*

9. *OT and building automation*
(i.e. heating and cooling, routers, switches)
- *As changes occur (real-time)*
- *Daily*
- *Weekly*
- *Monthly*
- *Quarterly*
- *Annually*
- *Never*
- *I don't know*

10. *Was cybersecurity discussed by the Trust Board within the last 12 months? Y/N*
- *What were the priorities discussed? (select all that apply)*
- *Keeping up with threat intelligence*
- *Medical device security*
- *Allocating cybersecurity spending*
- *Visibility of all assets connected to the network*
- *Staffing/recruitment*
- *Compliance with checking cybersecurity regulations/frameworks*
- *Securing the supply chain*
- *Dealing with ransomware*
- *IoT / OT Security*
- *Connected Chinese or Russian made devices*
- *Other:*

11. *How often is cybersecurity discussed by the board*

Every 3 months

- *every 6 months*
- *Every 12 months*
- *Ad hoc*
- *Never*

12. *Is medical device security a specific project on your roadmap for the next 12 months?*

13. *Are you able to respond to high severity NHS cyber alerts within the stated 48 hour timeline and patch within two weeks from disclosure?*

14. *What are the main challenges in meeting NHS Cyber Alert timelines?*

15. *What is your process for mapping individual NHS Cyber Alerts to every device on your network?*

16. *Are you identifying and removing Chinese made devices recently banned for sensitive areas by the British Government? How are you identifying them?*

17. *Does the Trust have enough resources to make sufficient investment to deal with replacing legacy and unsupported medical devices?*

18. *Are you able to attract and retain sufficient numbers of IT staff to fill available roles?*

19. *Do you feel you have sufficient IT staff to meet the demands placed upon you?*

20. *In the past year, has a cyberattack originated from a 3rd party vendor with access to your network (supply chain attack)? If so, what service did the 3rd party provide (not company names)?*