Freedom of Information Request

Reference Number: EPUT.FOI.23.2919
Date Received: 12th of April 2023

Information Requested:

1. What is your primary inventory method for tracking each device type connected to the network?

IT devices (i.e. pc, laptop)

- CMDB
- IoT (i.e smart Tvs, smart watches,, assistants like Alexa, Siri)
- Manual spreadsheet
- Connected Medical devices / IoMT (i.e. remote health monitoring devices, robotic surgery, imaging machines, MRI scanner)
- OT and building automation
- (i.e. heating and cooling, routers, switches)
- CMDB

As a mental health and community trust, we do not use devices of this nature. The exception being virtual ward remote monitoring technology which is asset managed though a third party CMDB

2. How often is the information on those systems updated?

IT devices (i.e. pc, laptop)

- As changes occur (real-time)
- IoT (i.e smart Tvs, smart watches,, assistants like Alexa, Siri)
- As changes occur (real-time)
- Connected Medical devices / IoMT (i.e. remote health monitoring devices, robotic surgery, imaging machines, MRI scanner)
- OT and building automation
- (i.e. heating and cooling, routers, switches)
- As changes occur (real-time)

Please see response to Question 1

3. Was cybersecurity discussed by the Trust Board within the last 12 months?

Yes

4. What were the priorities discussed? (select all that apply)

- Keeping up with threat intelligence
- Medical device security
- Compliance with checking cybersecurity regulations/frameworks
- Dealing with ransomware
- IoT / OT Security

All

5. How often is cybersecurity discussed by the board

Every 3 months

---

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

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

8. What are the main challenges in meeting NHS Cyber Alert timelines?
The unpredictable nature of any new threat emergence

9. What is your process for mapping individual NHS Cyber Alerts to every device on your network?
Realtime monitoring and compliance dashboards with an assurance reporting framework

10. Are you identifying and removing Chinese made devices recently banned for sensitive areas by the British Government? How are you identifying them?
This information is exempt under Section 31 (1a) of the Freedom of Information Act as disclosure would, or would be likely to, prejudice the prevention or detection of crime. Essex Partnership NHS Foundation Trust believe that releasing this information would enable cyber criminals to identify and take advantage of any weaknesses within the security of trust services. This would put patient & trust information at risk, including clinical, financial, and sensitive personal data. We therefore apply section 31(1)(a). Section 31 is a qualified exemption, so we have considered the public interest, but we believe that on this occasion the risk to data outweighs the public interest in cyber security concerns.

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

12. Are you able to attract and retain sufficient numbers of IT staff to fill available roles?
No, reliant on contractors to remain compliant

13. Do you feel you have sufficient IT staff to meet the demands placed upon you?
Yes

14. Approximately how long does it take for the Trust to assess on Data Security and Protection Toolkit (DSPT)? What takes the most time?
This information is exempt under Section 31 (1a) of the Freedom of Information Act as disclosure would, or would be likely to, prejudice the prevention or detection of crime. Essex Partnership NHS Foundation Trust believe that releasing this information would enable cyber criminals to identify and take advantage of any weaknesses within the security of trust services. This would put patient & trust information at risk, including clinical, financial, and sensitive personal data. We therefore apply section 31(1)(a). Section 31 is a qualified exemption, so we have considered the public interest, but we believe that on this occasion the risk to data outweighs the public interest in cyber security concerns.

15. 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)?
This information is exempt under Section 31 (1a) of the Freedom of Information Act as disclosure would, or would be likely to, prejudice the prevention or detection of crime.

Essex Partnership NHS Foundation Trust believe that releasing this information would enable cyber criminals to identify and take advantage of any weaknesses within the security of trust services. This would put patient & trust information at risk, including clinical, financial, and sensitive personal data. We therefore apply section 31(1)(a). Section 31 is a qualified exemption, so we have considered the public interest, but we believe that on this occasion the risk to data outweighs the public interest in cyber security concerns.

---

31 Law enforcement.

(1)Information which is not exempt information by virtue of section 30 is exempt information if its disclosure under this Act would, or would be likely to, prejudice—

(a)the prevention or detection of crime,

(b)the apprehension or prosecution of offenders,

(c)the administration of justice,

(d)the assessment or collection of any tax or duty or of any imposition of a similar nature,

(e)the operation of the immigration controls,

(f)the maintenance of security and good order in prisons or in other institutions where persons are lawfully detained,

(g)the exercise by any public authority of its functions for any of the purposes specified in subsection (2),

(h)any civil proceedings which are brought by or on behalf of a public authority and arise out of an investigation conducted, for any of the purposes specified in subsection (2), by or on behalf of the authority by virtue of Her Majesty's prerogative or by virtue of powers conferred by or under an enactment, or

(i)any inquiry held under the **[F1**Inquiries into Fatal Accidents and Sudden Deaths etc. (Scotland) Act 2016**]** to the extent that the inquiry arises out of an investigation conducted, for any of the purposes specified in subsection (2), by or on behalf of the authority by virtue of Her Majesty's prerogative or by virtue of powers conferred by or under an enactment.

(2)The purposes referred to in subsection (1)(g) to (i) are—

(a)the purpose of ascertaining whether any person has failed to comply with the law,

(b)the purpose of ascertaining whether any person is responsible for any conduct which is improper,

(c)the purpose of ascertaining whether circumstances which would justify regulatory action in pursuance of any enactment exist or may arise,

(d)the purpose of ascertaining a person's fitness or competence in relation to the management of bodies corporate or in relation to any profession or other activity which he is, or seeks to become, authorised to carry on,

(e)the purpose of ascertaining the cause of an accident,

(f)the purpose of protecting charities against misconduct or mismanagement (whether by trustees or other persons) in their administration,

(g)the purpose of protecting the property of charities from loss or misapplication,

(h)the purpose of recovering the property of charities,

(i)the purpose of securing the health, safety and welfare of persons at work, and

(j)the purpose of protecting persons other than persons at work against risk to health or safety arising out of or in connection with the actions of persons at work.

(3)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, prejudice any of the matters mentioned in subsection (1).

Publication Scheme:

As part of the Freedom of Information Act all public organisations are required to proactively publish certain classes of information on a Publication Scheme. A publication scheme is a guide to the information that is held by the organisation. EPUT's Publication Scheme is located on its Website at the following link https://eput.nhs.uk