Alder Hey Children's NHS
NHS Foundation Trust

Reference Number: FOIAH2324/017

From: Commercial

Date: 12 April 2023

Subject: Cyber Security and Network Devices

Q1

1. What is your primary inventory method for tracking each device type connected to the network?
   - i. IT devices (i.e. pc, laptop)
     - a. CMDB
     - b. Manual spreadsheet
     - c. Automated device detection
     - d. Other
     - e. None
   - ii. IoT (i.e smart Tvs, smart watches,, assistants like Alexa, Siri)
     - a. CMDB
     - b. Manual spreadsheet
     - c. Automated device detection
     - d. Other
     - e. None
   - iii. Connected Medical devices / IoMT (i.e. remote health monitoring devices, robotic surgery, imaging machines, MRI scanner)
     - a. CMDB
     - b. Manual spreadsheet
     - c. Automated device detection
     - d. Other
     - e. None
   - iv. OT and building automation
     - a. (i.e. heating and cooling, routers, switches)
     - b. CMDB
     - c. Manual spreadsheet
     - d. Automated device detection
     - e. Other
     - f. None

A1

- i. Automated device detection
- ii. None
- iii. CMDB
- iv. Other

Q2

2. How often is the information on those systems updated?
   - i. IT devices (i.e. pc, laptop)
     - a. As changes occur (real-time)
     - b. Daily
     - c. Weekly
     - d. Monthly

e. Quarterly
f. Annually
g. Never
h. I don't know

ii. IoT (i.e smart Tvs, smart watches,, assistants like Alexa, Siri)
a. As changes occur (real-time)
b. Daily
c. Weekly
d. Monthly
e. Quarterly
f. Annually
g. Never
h. I don't know

iii. Connected Medical devices / IoMT (i.e. remote health monitoring devices, robotic surgery, imaging machines, MRI scanner)
a. As changes occur (real-time)
b. Daily
c. Weekly
d. Monthly
e. Quarterly
f. Annually
g. Never
h. I don't know

iv. OT and building automation (i.e. heating and cooling, routers, switches)
a. As changes occur (real-time)
b. Daily
c. Weekly
d. Monthly
e. Quarterly
f. Annually
g. Never
h. I don't know

A2 i. Daily
ii. Information not held – the Trust does not routinely collate or hold this information centrally as part of its management or performance data.
iii. Annually - Dependent on frequency of maintenance
iv. Information not held – the Trust does not routinely collate or hold this information centrally as part of its management or performance data.

Q3 Was cybersecurity discussed by the Trust Board within the last 12 months? Y/N

A3 Yes

Q4 What were the priorities discussed? (select all that apply)
a. Keeping up with threat intelligence
b. Medical device security
c. Allocating cybersecurity spending
d. Visibility of all assets connected to the network
e. Staffing/recruitment

f. Compliance with checking cybersecurity regulations/frameworks
g. Securing the supply chain
h. Dealing with ransomware
i. IoT / OT Security
j. Connected Chinese or Russian made devices
k. Other:

A4 Compliance with checking cybersecurity regulations/frameworks

Q5 How often is cybersecurity discussed by the board

a. Every 3 months
b. every 6 months
c. Every 12 months
d. Ad hoc
e. Never

A5 Ad hoc

Q6 Is medical device security a specific project on your roadmap for the next 12 months?

A6 Yes, medical device security is being looked at

Q7 Are you able to respond to high severity NHS cyber alerts within the stated 48 hour timeline and patch within two weeks from disclosure?

A7 This will depend on the nature of the alert, however to date we have been able to meet the target deadlines

Q8 What are the main challenges in meeting NHS Cyber Alert timelines?

A8 Complexity of required resolutions, arranging required downtimes

Q9 What is your process for mapping individual NHS Cyber Alerts to every device on your network?

Q9 Our discovery tool has specific reports to identify vulnerable devices based on each alert

Q10 Are you identifying and removing Chinese made devices recently banned for sensitive areas by the British Government? How are you identifying them?

A10 We do not have a formal program as we did not purchase such devices historically, however we are able to use our network scanning tools to provide adhoc assurances regarding this.

Q11 Does the Trust have enough resources to make sufficient investment to deal with replacing legacy and unsupported medical devices?

Q11 Unsupported and Legacy devices are prioritised as part of the capital replacement plan.

Q12 Are you able to attract and retain sufficient numbers of IT staff to fill available roles?

A12 This will depend on the grade, skill set and timing of vacancies, however to date we have been able to fill required roles.

Q13 Do you feel you have sufficient IT staff to meet the demands placed upon you?

Q13 When additional resources requirements are required we are able to bring in temporary staff as required to cover these needs.

Q14 Approximately how long does it take for the Trust to assess on Data Security and Protection Toolkit (DSPT)? What takes the most time?

A14 Information not held. We do not record time spent on the Data Security and Protection Toolkit (DSPT).

Q15 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)?

A15 No