St Helens and Knowsley Teaching Hospitals NHS Trust

Ref no:	088210219
From:	Commercial
Date:	21/02/19
Subject:	Cybersecurity

REQUEST

Answers have been highlighted for the multiple choice questions.

1. Are you aware of the Minimum Cyber Security Standard, published 25th June 2018?
    a. Yes
    b. No

2. What is your annual dedicated budget for cybersecurity (including personnel and technology)?
    a. £10,000 or less
    b. £10,001 - £50,000
    c. £50,001 - £100,000
    d. £100,001 - £500,000
    e. £500,001 - £1,000,000
    f. £1,000,001 - £5,000,000
    g. £5,000,001 - £10,000,000
    h. £10,000,001 or more

3. Approximately how many cyber-attacks (of any kind) have you experienced in your organisation in these 12-month periods?

	None	1 – 50	50 – 100	100 – 200	200 – 500	500 -1000	1000+
1st January 2017 – 31st December 2017	X						
1st January 2018 – 31st December 2018	X						

4. Which of the following attack / cybersecurity threat types have been detected by your organisation? [Select all that apply]
    a. Hacking
    b. Phishing

c. Malware
d. Ransomware
e. Accidental/careless insider threat
f. Malicious insider threat
g. Foreign governments
h. Crypto mining
i. Other, please specify: _____

5. Which of the following form part of your cybersecurity defence technology strategy? [Select all that apply]

a. Firewall
b. Antivirus software
c. Network device monitoring
d. DNS filtering
e. Malware protection
f. Log management
g. Network configuration management
h. Patch management
i. Network traffic analysis
j. Multi-factor authentication
k. Network perimeter security solutions
l. Employee training (whole organisation)
m. Employee training (IT team)
n. Other, please specify: _____

6. Which of these obstacles has your organisation experienced in maintaining or improving IT security? [Select all that apply]

a. Competing priorities and other initiatives
b. Budget constraints
c. Lack of manpower
d. Lack of technical solutions available at my agency
e. Complexity of internal environment
f. Lack of training for personnel
g. Inadequate collaboration with other internal teams or departments
h. Other, please specify: _____

RESPONSE

The Trust must do its utmost to protect patient and staff information.

Patient information and staff information are the foundations upon which healthcare is built, and the Trust have a clear responsibility to safeguard this information to ensure we are able to provide the necessary care to our service users.

To provide the requested information above would highlight any vulnerability, should any such vulnerability exist (within hardware or software or architecture or Vendor, etc.), within our IT infrastructure which could be

exploited for the purposes of ransomware, other malware, or to withhold/disrupt IT functionality within the Trust.

This information relating to the cyber security agenda is likely to assist criminal offenders thereby seriously threatening the effective delivery of healthcare by the Trust. The act of gathering information as requested, in the hacking arena is known as foot-printing and our network architecture is closely protected to at least NHS protect if not NHS Confidential. Therefore:

Our patients (and staff) must have confidence that their very sensitive personal data will be held securely.

They (patients & staff) must have confidence that we'll be able to provide the services they need.

Therefore, providing the specific requested information would put their confidence at risk.

Furthermore, loss of patient and staff data by such an attack would massively impact upon our ability to provide effective healthcare to our service users.

And therefore, this would be extremely harmful to the public & the services the Trust provides.

Therefore in accordance with Section 31 of the Freedom of Information Act the Trust will not be releasing the requested information as this would prejudice our ability to resist cyber-attacks.