NHS
Lancashire & South Cumbria
NHS Foundation Trust

FOI Request Response information

FOI request reference:	2019/081
Date request received:	20/02/2019
Date request responded to:	13/03/2019
Category:	IM&T
Tags:	Cyber, security, standard, budget, technology, personnel, staff, cyber-attack, malware, phishing, ransomware, anti-virus,

Request Detail:

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							
1st January 2018 – 31st December 2018							

NHS
Lancashire & South Cumbria
NHS Foundation Trust

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 Detail:

1. Are you aware of the Minimum Cyber Security Standard, published 25th June 2018?

a. Yes
b. No

Lancashire & South Cumbria NHS Foundation Trust

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: _____

We have considered your request for the above information and regrettably are not able to provide this to you. It is Trust policy that as this information could lead to potential exploitation of our IT systems and equipment as well as any vulnerabilities which could result in a possible Cyber Attack or compromise of the systems, equipment or wider NHS infrastructure we do not release this information at all.

In assessing your request for this information we have considered that section 24 of the Freedom of Information Act. Section 24(1) of the act states that "Information which does not fall within section 23(1) is exempt information if exemption from section 1(1)(b) is required for the purpose of safeguarding national security."

In all the circumstances we are of the opinion that to provide this information would have the potential to compromise National Security and more particularly National Cyber Security.

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: _____

We have considered your request for the above information and regrettably are not able to provide this to you. It is Trust policy that as this information could lead to potential exploitation of our IT systems and equipment as well as any vulnerabilities which could result in a possible Cyber Attack or compromise of the systems, equipment or wider NHS infrastructure we do not release this information at all.

In assessing your request for this information we have considered that section 24 of the Freedom of Information Act. Section 24(1) of the act states that "Information which does not fall within section 23(1) is exempt information if exemption from section 1(1)(b) is required for the purpose of safeguarding national security."

In all the circumstances we are of the opinion that to provide this information would have the potential to compromise National Security and more particularly National Cyber Security.

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: _____

We have considered your request for the above information and regrettably are not able to provide this to you. It is Trust policy that as this information could lead to potential exploitation of our IT systems and equipment as well as any vulnerabilities which could result in a possible Cyber Attack or compromise of the systems, equipment or wider NHS infrastructure we do not release this information at all.

In assessing your request for this information we have considered that section 24 of the Freedom of Information Act. Section 24(1) of the act states that “Information which does not fall within section 23(1) is exempt information if exemption from section 1(1)(b) is required for the purpose of safeguarding national security.”

In all the circumstances we are of the opinion that to provide this information would have the potential to compromise National Security and more particularly National Cyber Security.