March 20 2019
Reference no.18190436

Dear

Request for Information: Freedom of Information Act

Thank you for your email of 20th February making a request for information under the Freedom of Information Act. You requested the following information and the Trust is able to provide the information below in response:

Request:

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							

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:

1. Are you aware of the Minimum Cyber Security Standard, published 25th June 2018?
   a. <mark>Yes</mark>
   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? The Trust does not hold this information.

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

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: _____

If you are unhappy with the service you have received in relation to your request and wish to make a complaint or request a review of our decision, you should write to me and I will ensure the decision is reviewed. The Trust will consider undertaking a review if requested to do so within 40 working days of the date the response is received by the applicant, and will apply discretion if a longer period of time has passed.

Should you wish to make a complaint as a result of the outcome of such a review, you may apply directly to the Information Commissioner's Office (ICO) for a decision.

Generally, the ICO cannot make a decision unless you have exhausted the complaints procedure provided by the Trust for FoI Act matters.

The ICO can be contacted at:

The Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF

Please contact me if there are any further queries.

Kind regards,

Yours sincerely,

Mark Underwood

Head of Information Governance