The Tavistock and Portman NHS
NHS Foundation Trust

Freedom of Information Act 2000 disclosure log entry

Reference

16-17357

Date sent

15/03/2017

Subject

Cyber Attacks and Cyber Security

Details of enquiry

1. Has your organisation completed all of the government's '10 steps to cyber security'?
    - Yes
    - No

2. Have you suffered Distributed Denial of Service (DDoS) cyber attacks on your network in the last year?
    - Yes
    - No

3. If so, how many DDoS attacks did you experience during 2016?
    a. Attacks occur weekly or even daily
    b. Attacks occur monthly
    c. Less than a handful of attacks during the entire year

4. Has your organisation ever been the victim of a DDoS attack which was used in combination with another type of cyber attack, such as a demand for ransom/ransomware, network infiltration or data theft?
    - Yes
    - No

5. How does your IT team detect that your organisation has suffered a DDoS attack?
    - End-users complain of a service issue
    - High bandwidth spikes with other network security tools
    - Infrastructure outages/failures, (e.g. firewalls went down)
    - Application failures, eg. Websites going down

6. Does your method of DDoS mitigation detect sub-saturating DDoS attacks of less than 30 minutes in duration, which do not typically overwhelm the network?

○ Yes
○ No

Response Sent

7. Has your organisation completed all of the government’s ’10 steps to cyber security’?

   ~~○ Yes~~
   ○ **No**

8. Have you suffered Distributed Denial of Service (DDoS) cyber attacks on your network in the last year?

   ~~○ Yes~~
   ○ **No**

9. If so, how many DDoS attacks did you experience during 2016?

   d. Attacks occur weekly or even daily
   e. Attacks occur monthly
   f. Less than a handful of attacks during the entire year
   Not applicable

10. Has your organisation ever been the victim of a DDoS attack which was used in combination with another type of cyber attack, such as a demand for ransom/ransomware, network infiltration or data theft?

    ~~○ Yes~~
    ○ **No**

11. How does your IT team detect that your organisation has suffered a DDoS attack?

    ~~○ End-users complain of a service issue~~
    ○ ~~High bandwidth spikes with other network security tools~~
    ~~○ Infrastructure outages/failures, (e.g. firewalls went down)~~
    ○ **Application failures, eg. Websites going down**

12. Does your method of DDoS mitigation detect sub-saturating DDoS attacks of less than 30 minutes in duration, which do not typically overwhelm the network?

    ~~○ Yes~~
    ~~○ No~~
    ○ **Don’t know**