FOI Request Response information

FOI request reference:	2017/090
Date request received:	15/03/2017
Date request responded to:	20/03/2017
Category:	IM&T
Tags:	Cyber, security, attacks

Request Detail:

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

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

5. How does your IT team detect that your organisation has suffered a DDoS attack?
    - o End-users complain of a service issue
    - o High bandwidth spikes with other network security tools
    - o Infrastructure outages/failures, (e.g. firewalls went down)
    - o 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?
    - o Yes
    - o No

Response Detail:

The Trust response to your recent FOI request is as follows:

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

   No

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

   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

   c

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

   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

   All

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

   No