

Freedom of Information Response

Date: 17 March 2017
Log no: FOI 871

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

Our Trust's ICT is outsourced to a third party.

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

Our Trust's ICT is outsourced to a third party.

