

Date: 28/03/2017

FREEDOM OF INFORMATION REQUEST FOI/013351 – Cyber security

I am writing to make a request for information under the Freedom of Information Act 2000.

Exemption 43 (2) applied given the organisation considers this level of information commercially sensitive from an information security perspective.

The public interest test set out in section 2(2)(b) supports application of exemption 43 (2) given there is a greater public interest in maintaining the exemption 43 (2) outweighing the public interest in disclosure in order to protect public and public services against cyber security threats.

Has your organisation completed all of the government's '10 steps to cyber security' - Exemption 43

- Yes
- No

Have you suffered Distributed Denial of Service (DDoS) cyber attacks on your network in the last year - Exemption 43

- Yes
- No

If so, how many DDoS attacks did you experience during 2016 - Exemption 43

- a. Attacks occur weekly or even daily
- b. Attacks occur monthly
- c. Less than a handful of attacks during the entire year

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? - Exemption 43

- Yes
- No

How does your IT team detect that your organisation has suffered a DDoS attack? - Exemption 43

- 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

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? - Exemption 43

- Yes
- No