FOI_0577_21/22 – FOI request concerning – Information Technology Security

1. Do you have a formal IT security strategy? (Please provide a link to the strategy)

No – not a present

2. Does this strategy specifically address the monitoring of network attached device configurations to identify any malicious or non-malicious change to the device configuration?

N/A

3. If yes to Question 2, how do you manage this identification process – is it:

A. Totally automated – all configuration changes are identified and flagged without manual intervention.
B. Semi-automated – it's a mixture of manual processes and tools that help track and identify configuration changes.
C. Mainly manual – most elements of the identification of configuration changes are manual.

N/A

4. Have you ever encountered a situation where user services have been disrupted due to an accidental/non malicious change that had been made to a device configuration?

No

5. If a piece of malware was maliciously uploaded to a device on your network, how quickly do you think it would be identified and isolated?

A. Immediately
B. Within days
C. Within weeks
D. Not sure

To ensure the security of our systems and to not divulge information that could assist cyber attackers, we are not able to answer this question

6. How many devices do you have attached to your network that require monitoring?

A. Physical Servers: record number
B. PC's & Notebooks: record number

To ensure the security of our systems and to not divulge information that could assist cyber attackers, we are not able to answer this question

7. Have you ever discovered devices attached to the network that you weren't previously aware of?

No

8. If yes, how do you manage this identification process – is it:

A. Totally automated – all device configuration changes are identified and flagged without manual intervention.
B. Semi-automated – it's a mixture of manual processes and tools that help track and identify unplanned device configuration changes.
C. Mainly manual – most elements of the identification of unexpected device configuration changes are manual.

N/A

9. How many physical devices (IP's) do you have attached to your network that require monitoring for configuration vulnerabilities?

To ensure the security of our systems and to not divulge information that could assist cyber attackers, we are not able to answer this question

10. Have you suffered any external security attacks that have used malware on a network attached device to help breach your security measures?

Never

11. Have you ever experienced service disruption to users due to an accidental, non-malicious change being made to device configurations?

Never

12. When a scheduled audit takes place for the likes of PSN or Cyber Essentials, how likely are you to get significant numbers of audit fails relating to the status of the IT infrastructure?

A. Never
B. Occasionally
C. Frequently
D. Always

This is a matter of opinion and therefore not covered under the Freedom of Information Act