35196

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

Yes/No

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

Yes/No/Don't know

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

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

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?

Yes/No/Don't know

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?

Immediately/Within days/Within weeks/Not sure

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

Physical Servers:
PC's & Notebooks:

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

Yes/No

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

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

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

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

Have you ever experienced service disruption to users due to an accidental, non-malicious

change being made to device configurations?

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?

In line with advice from the National Cyber Security Centre, we do not provide information relating to hardware, software and systems and therefore, unfortunately, it is not possible to provide you with the information you have requested on this occasion.

By placing information about our systems into the public domain we would potentially be putting our IT framework at risk. This would prejudice substantially the Council's ability to effectively carry out its business if its IT framework were compromised as a consequence of the disclosure of this information.