Bath & North East Somerset Council
Request for Information

Requested information:

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

A) Yes

B) No

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?

A) Yes

B) No

C) Don't know

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.

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?

A) Yes

B) No

C) Don’t know

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

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

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

A) Yes

B) No

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.

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

Record Number:

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

A) Never

B) Not in the last 1-12 months

C) Not in the last 12-36 months

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

change being made to device configurations?

A) Never

B) Not in the last 1-12 months

C) Not in the last 12-36 months

11. 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

Response

We can confirm that we do not routinely provide details relating to IT Security due to the impact that this can have on the security of Council IT systems. As a result we have identified that section 43 of the Act is engaged. (Commercial Interests)

Although the Council aim to be transparent and accountable to the public, we must ensure that we do not provide information which if disclosed into the public domain, could prejudice IT security. The Council operates the majority of its services with a high dependency on its ICT support. Many services operate almost exclusively via information on databases, and most officers use electronic systems in daily working. An interruption of these systems, even for short period of maintenance, has considerable implications for the operation of services across the authority. While business continuity and disaster recovery processes exist, the Council would be foolish to invite damage to its systems by wilfully publicising information which could lead to any such interruption. It is therefore our view that the public interest in withholding this information to prevent the prejudice to the Council's service were it to be misused outweighs the public interest in supplying it.