EAST CAMBRIDGESHIRE DISTRICT COUNCIL
THE GRANGE, NUTHOLT LANE,
ELY, CAMBRIDGESHIRE CB7 4EE
Telephone: Ely (01353) 665555
DX41001 ELY Fax: (01353) 665240
www.eastcambs.gov.uk

Further to your information request FOI/EIR 21/22-294 please find your question and our response below.

Request:

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:
1.No

2. n/a

3. n/a

4. Information Refused Under Section 31

5. Information Refused Under Section 31

6. Information Refused Under Section 31

7. Information Refused Under Section 31

8. Information Refused Under Section 31

9. Information Refused Under Section 31

10. Information Refused Under Section 31

11. Information Refused Under Section 31

In respect of those requests that where answered in full or partially and the total refused please take this as notice under FOIA, that we:
a) Consider the information as exempt from disclosure under the Act;
b) Claim exempt under sections of the Act:
Section 31(1)(a) of the Freedom of Information Act 2000
c)State why the exemption applies:
31 Law enforcement.
(1) Information which is not exempt information by virtue of section 30 is exempt information ifits disclosure under this Act would, or would be likely to, prejudice (a)the prevention or detection of crime

We can neither confirm nor deny whether we hold this information. Section 31(1)(a) exempts informationif its disclosure under this Act would prejudice the prevention or detection of crime. By

confirming or denying whether we hold information of this type, this could in itself disclose information which would, orwould be likely to, prejudice the prevention or detection of crime.

This exemption covers all aspects of the prevention and detection of crime, including public authoritieswithout any specific law enforcement responsibilities. The exemption can be used not only to withhold information provided to a law enforcement agency, but also to withhold information that would make anyone, including the public authority itself, more vulnerable to crime. Further guidance on section 31can be found here:
https://ico.org.uk/media/for-organisations/documents/1207/law-enforcement-foi-section-31.pdf

As Section 31(1)(a) is a qualified exception, we, the authority, must consider the balance of public interestin the circumstances of the request.
Arguments in favour of disclosing the information:

- There is public interest in the Council's accountability and transparency.

Arguments in favour of withholding the information:

- While there may be public interest in knowing this information, the ICT Department considers that providing the requested information would, or would be likely to, substantially prejudice and present asignificant risk to the security arrangements in place to protect the network as well as information and data held by our Council.
- Disclosure of information relating to ICT security puts the Council at risk of a malicious hacking attack. This would compromise the Council's ability to provide its services and carry out 'business-as-usual' should our systems be compromised. Were our systems to be compromise, the cost of a system recoverywould be detrimental to the Council's commercial interests.
- There is an overwhelming public interest in keeping the Council's computer systems secure which wouldbe served by non-disclosure.

Whilst the Council strongly believes in the principle of open and accountable local government, the public interest in maintaining the exception outweighs the public interest in disclosing the information.

This concludes your request FOI/EIR 21/22-294

If information has been refused please treat this as a Refusal Notice for the purposes of the Act.

If you disagree with our decision or are otherwise unhappy with how we have dealt with your request in the first instance you may approach foi@eastcambs.gov.uk and request a review. A request for review must be made in no more than 40 working days from the date of this email.

Should you remain dissatisfied with the outcome you have a right under s50 of the Freedom of Information Act to appeal against the decision by contacting the Information Commissioner, Wycliffe House, Water Lane, Wilmslow SK9 5AF.