INFORMATION GOVERNANCE
Lafrowda House
St. German's Road
Exeter, UK
EX4 6TL
informationgovernance@exeter.ac.uk
www.exeter.ac.uk/ig

11 January 2022

Ref: FOI21 - 0534

Dear Requester,

Thank you for your email of 16th December 2021 requesting information under the Freedom of Information Act 2000. Please see the responses to each of your questions below:

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

For questions 1 – 11 It is the view of the University of Exeter that compliance with your request is exempt under the Freedom of Information Act 2000 Section 31(1)a and 31(3) – Prejudice the prevention or detection of crime and Section 43 (2) – prejudice the commercial interests of the University.

The University takes the security its networks and the risk of cyber-attacks very seriously and we can confirm we have appropriate controls in place to protect our network. There are a number of sites and content types, which are blocked to protect the network and users of our systems. Consequently, the University can neither confirm nor deny if data relating to the monitoring or statistics is held. As a University with a strong focus on academic freedom we have processes in place to allow access to these sources and materials should there be sufficient academic grounds to do so. This process is managed as a partnership between Information Governance, Research Ethics and Exeter IT.

It is the view of the University that providing information relating to the nature of the security measures in place on our networks could be used to threaten University information systems. In the current climate, we are compelled to mitigate as much as possible the risks posed by cybercrime. In addition providing this information would prejudice commercial interests, as it would increase risk to our security and therefore our ability to operate as a commercial entity in the context of securing funding for related activities.

As the above exemptions are qualified, we are required to undertake a public interest test to examine if the public interest favouring disclosure outweighs the public interest in withholding it. In favour of disclosure, we considered the principles of both transparency and accountability in the way a public authority performs its functions. Opposing this we considered the factors favouring the withholding the information and this specifically relates to the nature of the exemption concerning the prevention or detection of crime and the University's ability to operate as a commercial entity. There is a substantial public interest in protecting society from the impact of crime and not facilitating any steps, which are likely to prejudice the prevention or detection of crime. Furthermore, there is a substantial public interest in not jeopardising the University's resilience to cyber threats given the likelihood of an attack. Our assessment is that in all the circumstances of the case, the public interest in maintaining the integrity of our systems outweighs the public interest in disclosing the requested information.

This response has been prepared in accordance with a request received pursuant to the Freedom of Information Act 2000. The supply of documents under FOI does not give the person who receives the information an automatic right to re-use the documents without obtaining the consent of the copyright holder. If you are dissatisfied with the handling of your request, you have the right to ask for an internal review. You must submit this to the Information Governance Office in writing within 40 days of receipt of this notification. Please quote the reference number above.

If you are not content with the outcome of the internal review, you have the right to apply directly to the Information Commissioner for a decision. The Information Commissioner can be contacted at: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF. (https://ico.org.uk/)

Kind Regards,

Information Governance

University of Exeter