UK Research and Innovation

[redacted]

5 January 2022

Dear [redacted],

Freedom of Information request: FOI2021/00507

Thank you for your Freedom of Information request received on the 29 November in which you requested the following:

Your request:

I am writing to make an open government request for all the information to which I am entitled under the Freedom of Information Act 2000.

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

Our response:

I can confirm UK Research and Innovation (UKRI) hold some of the information relevant to your request. Please see the information below.

UK Research and Innovation brings together seven Research Councils, (AHRC, BBSRC, EPSRC, ESRC, MRC, NERC and STFC), Innovate UK and Research England. As you sent the same query to multiple councils, they have been amalgamated into one request.

Information in response to your questions is as follows:

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

A) Yes

Releasing the UKRI IT Security Strategy and details of what it contains would prejudice the prevention or detection of crime as per Section 31(1)(a) of the Freedom of Information Act.

Section 31(1)(a) is a qualified exemption and therefore subject to a public interest test. UKRI applied the Public Interest Test to this request as set out below;

Public interest in favour of disclosure:

- There is a public interest in favour of release of the information, to uphold the principles of transparency and accountability, in disclosing information about government or public authority infrastructure and contracts

Public interest test in favour of withholding the information:

- The release of this information would make UKRI more vulnerable to crime
- The crime in question would be a malicious attack on UKRI's computer infrastructure and/or systems
- The release of this information would be seen to prejudice the prevention or detection of crime, by making UKRI's computer systems more vulnerable to hacking and therefore facilitate the possibility of a criminal offence being carried out
- There is an overwhelming public interest in keeping government or public authority computer systems secure, which would be served by non-disclosure.

UKRI has therefore reached the conclusion that, on balance, the public interest is better served by withholding the selected information under Section 31(1)(a).

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?

Please see the response to Q1.

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

Please see the response to Q1.

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

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?

This question is outside of the scope of FOI as it is asking for commentary or opinion, rather than for information that is held.

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

We estimate that the cost of complying with this section of your request would exceed the appropriate statutory limit as specified within Section 12 of the FOIA which for UKRI is set at £450. This represents the estimated cost of 18 hours of staff resource on locating, retrieving and extracting the information.

To gather this information, we have determined that it would be necessary to go to 22 different parts of UKRI and interrogate multiple asset registers, due to the devolved management of assets within the organisation. This is a process that has been estimated by our IT staff to take substantially more than the 18 hour limit.

Consequently, UKRI is not obliged under Section 12 of the FOIA to process this section of your request further.

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

A) Yes

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

B) Semi-automated – it's a mixture of manual processes and tools that help track and identify unplanned device configuration changes.

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

Please see the response to Q6.

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

None of the available answers are relevant to UKRI.

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

None of the available answers are relevant to UKRI.

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?

This question is outside of the scope of FOI as it is asking for commentary or opinion, rather than for information that is held.

If you have any queries regarding our response or you are unhappy with the outcome of your request and wish to seek an internal review of the decision, please contact:

Head of Information Governance
Email: foi@ukri.org or infogovernance@ukri.org

Please quote the reference number above in any future communications.

If you are still not content with the outcome of the internal review, you may apply to refer the matter to the Information Commissioner for a decision. Generally, the ICO cannot make a decision unless you have exhausted the review procedure provided by UKRI. The Information Commissioner can be contacted at: http://www.ico.gov.uk/

If you wish to raise a complaint regarding the service you have received or the conduct of any UKRI staff in relation to your request, please see UKRI's complaints policy: https://www.ukri.org/about-us/policies-and-standards/complaints-policy/

Yours sincerely,

[redacted]
Information Governance
Information Rights Team
UK Research and Innovation
foi@ukri.org | dataprotection@ukri.org