Freedom of Information (FOI) Request
Received: 29 November 2021

Published: www.theccc.org.uk/about/transparency

Climate Change Committee
1 Victoria Street,
Westminster, London,
SW1H 0ET
w theccc.org.uk

Date: 04 January 2022
Ref: Sent by email from communications@theccc.org.uk

Your request:

Thank you for your request for information of 29 November 2021 about Information Technology for the Climate Change Committee. We have handled your request under the Freedom of Information Act 2000 (FOIA).

Your information request and our response are set out 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*

Our response:

The CCC procures its IT services from the Department for Environment and Rural Affairs (Defra) and the following response has been provided by them:

The response to part 1 of your request is 'yes'.

The remainder of the information you have requested is being withheld as it falls under the exemption in section 31(1)(a) of the FOIA, which relates to the prevention or detection of crime. In applying this exemption, we have had to balance the public interest in disclosing the information, against the public interest in withholding it.

We recognise that there is a public interest in disclosure of information around network infrastructure and cyber vulnerabilities, as this will promote openness and transparency within Government, and also show whether the functions of Government are adequately protected from cyber-attacks.

However, there is a strong public interest in withholding this information, as it could aid potential attackers by revealing any potential network infrastructure / cyber vulnerabilities which could provide the information necessary to consider mounting a possible attack. Any attempt to carry out a cyber-attack against an IT system is a criminal offence. Providing detailed information in this area would assist someone in testing the effectiveness of the Climate Change Committee's defences against such attacks and could also assist a criminal to deduce if their attacks had been detected or thwarted.

This exemption is engaged because releasing the information will prejudice the prevention of crime by facilitating the possibility of a criminal offence being carried out. Releasing information which can be used to aid or plan a cyber-attack is withheld and we apply this rule across all government departments as it would have detrimental impacts to the running of public services.

We have therefore decided that the information should be withheld.

Information disclosed in response to this FOIA request is releasable to the public. In keeping with the spirit and effect of the FOIA and the government's Transparency Agenda, this letter and the information disclosed to you may be placed on the CCC website, together with any related information that will provide a key to its wider context. No information identifying you will be placed on the CCC website.

If you are dissatisfied with the handling of your request, you have the right to ask for an internal review. If you are not content with the outcome of the review, you may apply directly to the Information Commissioner for a decision. In keeping with our transparency policy, the information released to you will be published on www.theccc.org.uk. Please note that this publication will not include your personal data.

Kind regards,
Climate Change Committee