Climate Change Committee

The UK's independent adviser on tackling climate change

Freedom of Information (FOI) Request
Received: 31st August 2021

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

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

Date: 24th September 2021,
Ref: Sent by email from communications@theccc.org.uk

Your request:

1. *In the past three years has your organisation:*

a. Had any ransomware incidents? (An incident where an attacker attempted to, or successfully, encrypted a computing device within your organisation with the aim of extorting a payment or action in order to decrypt the device?)

i. If yes, how many?

b. Had any data rendered permanently inaccessible by a ransomware incident (i.e. some data was not able to be restored from back up.)

c. Had any data rendered permanently inaccessible by a systems or equipment failure (i.e. some data was not able to be restored from back up.)

d. Paid a ransom due to a ransomware incident / to obtain a decryption key or tool?

i. If yes was the decryption successful, with all files recovered?

e. Used a free decryption key or tool (e.g. from https://www.nomoreransom.org/)?

i. If yes was the decryption successful, with all files recovered?

f. Had a formal policy on ransomware payment?

i. If yes please provide, or link, to all versions relevant to the 3 year period.

g. Held meetings where policy on paying ransomware was discussed?

h. Paid consultancy fees for malware, ransomware, or system intrusion investigation

i. If yes at what cost in each year?

i. Used existing support contracts for malware, ransomware, or system intrusion investigation?

j. Requested central government support for malware, ransomware, or system intrusion investigation?

k. Paid for data recovery services?

i. If yes at what cost in each year?

l. Used existing contracts for data recovery services?

m. Replaced IT infrastructure such as servers that have been compromised by malware?

i. If yes at what cost in each year?

n. Replaced IT endpoints such as PCs, Laptops, Mobile devices that have been compromised by malware?

i. If yes at what cost in each year?

o. Lost data due to portable electronic devices being mislaid, lost or destroyed?

i. If yes how many incidents in each year?

The information you have requested is being withheld as it falls under the exemption in section 31(3) of the FOIA, which relates to the prevention or detection of crime. Please see below for more details.

2. Does your organisation use a cloud based office suite system such as Google Workspace (Formerly G Suite) or Microsoft's Office 365?

We can confirm that we use Microsoft Office 365.

a. If yes is this system's data independently backed up, separately from that platform's own tools?

The information you have requested is being withheld as it falls under the exemption in section 31(3) of the FOIA, which relates to the prevention or detection of crime. Please see below for more details.

3. Is an offsite data back-up a system in place for the following? (Offsite backup is the replication of the data to a server which is separated geographically from the system's normal operating location site.)

a. Mobile devices such as phones and tablet computers

b. Desktop and laptop computers

c. Virtual desktops

d. Servers on premise

e. Co-located or hosted servers

f. Cloud hosted servers

g. Virtual machines

h. *Data in SaaS applications*

i. *ERP / finance system*

j. *We do not use any offsite back-up systems*

The information you have requested is being withheld as it falls under the exemption in section 31(3) of the FOIA, which relates to the prevention or detection of crime. Please see below for more details.

4. *Are the services in question 3 backed up by a single system or are multiple systems used?*

The information you have requested is being withheld as it falls under the exemption in section 31(3) of the FOIA, which relates to the prevention or detection of crime. Please see below for more details.

5. *Do you have a cloud migration strategy? If so is there specific budget allocated to this?*

We can confirm that we have an internal cloud migration strategy, and that it has a dedicated budget allocated to it.

6. How many Software as a Services (SaaS) applications are in place within your organisation?

The CCC uses the Defra IT service. The Defra Digital, Data and Technology Services function manages around 80 SaaS applications on behalf of the Defra group.

a. How many have been adopted since January 2020?

The information you have requested is not held by Defra, who manage the CCC IT service.

Section 31(3) of the FOIA (Prevention or detection of crime)

For questions 1, 2a, 3 and 4 above, the information you have requested falls under the exemption in section 31(3) of the FOIA, which relates to the prevention or detection of crime. We have applied section 31(3) which removes the CCC's duty in section 1(1)(a) of the FOIA to tell you whether we hold the requested information. We can therefore neither confirm nor deny that CCC holds the information falling within the description specified in your request. This statement should not be taken as an indication that the information you requested is or is not held by the CCC.

In applying this exemption, we have had to balance the public interest in providing the neither confirm nor deny response.

We recognise that there is a public interest in confirming whether information exists concerning ransomware incidents in a government organisation. We understand that information on this area would promote openness and transparency.

However, there is a stronger public interest in neither confirming nor denying whether this information exists as it could aid malicious parties in attempts to attack the IT systems concerned. Revealing whether or not we have incurred any

ransomware incidents could provide information to a potential cyber attacker on an organisation's capabilities to respond and defend against attacks. Any attempt to carry out a cyberattack against an IT system is a criminal offence. This exemption is engaged because either confirming or denying such information is held will prejudice the prevention of crime by facilitating the possibility of a criminal offence being carried out. Such confirmation can be used to aid or plan a cyber-attack and it would potentially have detrimental impact to the running of public services.

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