FOI Ref	Response sent
9610	**3 Sep 2021**

(CCC) IT Security

Thank you for your request for information, which we have dealt with under the terms of the Freedom of Information Act 2000.

I hope the following will answer your query:

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? None

b. Had any data rendered permanently inaccessible by a ransomware incident (i.e., some data was not able to be restored from back up.) None

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.) None

d. Paid a ransom due to a ransomware incident / to obtain a decryption key or tool? None

i. If yes was the decryption successful, with all files recovered? None

e. Used a free decryption key or tool (e.g. from https://www.nomoreransom.org/)? None

i. If yes was the decryption successful, with all files recovered? None

f. Had a formal policy on ransomware payment? None

i. If yes please provide, or link, to all versions relevant to the 3 year period. None

g. Held meetings where policy on paying ransomware was discussed? None

h. Paid consultancy fees for malware, ransomware, or system intrusion investigation None

i. If yes at what cost in each year? None

i. Used existing support contracts for malware, ransomware, or system intrusion investigation? None

j. Requested central government support for malware, ransomware, or system intrusion investigation? None

k. Paid for data recovery services? None

i. If yes at what cost in each year? None

l. Used existing contracts for data recovery services? None

m. Replaced IT infrastructure such as servers that have been compromised by malware? None

i. If yes at what cost in each year? None

n. Replaced IT endpoints such as PCs, Laptops, Mobile devices that have been compromised by malware? None

i. If yes at what cost in each year? None

o. Lost data due to portable electronic devices being mislaid, lost or destroyed? None

i. If yes how many incidents in each year? None

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

a. If yes is this system's data independently backed up, separately from that platform's own tools? No

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 None

b. Desktop and laptop computers None

c. Virtual desktops Yes

d. Servers on premise Yes

e. Co-located or hosted servers Yes

f. Cloud hosted servers Yes

g. Virtual machines Yes

h. Data in SaaS applications None

i. ERP / finance system Yes

FOI Ref	Response sent
9610	**3 Sep 2021**

j. We do not use any offsite back-up systems N/A

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

5. Do you have a cloud migration strategy? If so, is there specific budget allocated to this? Not at this time

6. How many Software as a Services (SaaS) applications are in place within your organisation? a. How many have been adopted since January 2020? 2

Further queries on this matter should be directed to foi@cambridge.gov.uk