FOI_0477_21/22 – FOI request concerning – Ransomware Incidents

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?)

No

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

No

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.)

No

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

No

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

No

f) Had a formal policy on ransomware payment?

No

g) Held meetings where policy on paying ransomware was discussed?
No

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

No

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

Yes

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

No

k) **Paid for data recovery services?**

No

l) **Used existing contracts for data recovery services?**

Yes

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

No

n) **Replaced IT endpoints such as PCs, Laptops, Mobile devices that have been compromised by malware?**
N/A

i. **If yes at what cost in each year?**

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

No

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

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

Microsoft Office 365

With regards to Questions 3 - 6. This part of your request has been reviewed and unfortunately at this time, we are unable to provide the information being requested, as it has been exempt in accordance with Section 43(2) of the Freedom of Information Act 2000.

- Section 43(2) exempts information whose disclosure would, or would be likely to, prejudice the commercial interests of any person (an individual, a company, the public authority itself or any other legal entity).
- A public authority may refuse to confirm or deny that it holds information where such confirmation or denial in itself would (or would be likely to) prejudice those commercial interests.
- The section 43 exemptions are qualified exemptions, subject to the public interest test, which can be found https://www.solent.nhs.uk/about-us/trust-information/fois-released/ under the "Key Projects of Interest section".
- Please note the consultation period is expected to last until at least December 2021, at which point you are free to resubmit your request.

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

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

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

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