Liverpool Heart and Chest Hospital NHS
NHS Foundation Trust

Reference Number: FOI2021/303
From: Commercial

Date: 31 August 2021

Subject: Ransomware incidents, cloud based office suite system, offsite data back-up system, cloud migration strategy and Software as a Services (SaaS) applications

Q1 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?

A1
a. No
b. No
c. No
d. No
e. No
f. We have assessed the public interest in disclosure and believe the whilst factors for release would be openness and transparency, however the factors against release clearly outweigh this as release of the information would place the Trusts information systems and other related assets at risk of attack if released in to the public domain. We exempt the provision of this information under Section 24(1) - 'required for the purpose of safeguarding national security'. Our rationale for the application of this exemption is that the NHS is part of the nation's Critical National Infrastructure – as defined by the Centre for the Protection of National Infrastructure. Therefore we will not disclose information which may, in our opinion, weaken our state of readiness to cyber threats, as providing such detail on our operating systems may put in jeopardy these very systems, therefore, protection of our digital assets outweighs consideration of disclosure.
g. As per A1f.
h. No
i. No, however the Trust maintains a number of anti-intrusion systems and measures which provide points of investigation as required
j. No
k. No
l. No
m. No
n. No
o. We have not had any incidents of data being permanently lost due to portable electronic devices being mislaid, lost or destroyed in this time period

Q2 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?

A2 We have assessed the public interest in disclosure and believe the whilst factors for release would be openness and transparency, however the factors against release clearly outweigh this as release of the information would place the Trusts information systems and other related assets at risk of attack if released in to the public domain. We exempt the provision of this information under Section 24(1) - 'required for the purpose of safeguarding national security'. Our rationale for the application of this exemption is that the NHS is part of the nation's Critical National Infrastructure – as defined by the Centre for the Protection of National Infrastructure. Therefore we will not disclose information which may, in our opinion, weaken our state of readiness to cyber threats,

as providing such detail on our operating systems may put in jeopardy these very systems, therefore, protection of our digital assets outweighs consideration of disclosure.

Q3 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

Q4 Are the services in question 3 backed up by a single system or are multiple systems used?

A3-A4 We exempt the provision of this information under Section 24(1) - 'required for the purpose of safeguarding national security', as per A2. However the trust seeks to be compliant to the National Cyber Security Centre's guidance regarding backup provision where ever possible, which includes the requirement for multiple copies.

Q5 Do you have a cloud migration strategy? If so is there specific budget allocated to this?

A5 No cloud migration strategy, if systems were to be moved to cloud hosting they would be subject to separate planning.

Q6 How many Software as a Services (SaaS) applications are in place within your organisation?

a. How many have been adopted since January 2020?

A6 One

a. Zero