St Helens and Knowsley Teaching Hospitals NHS Trust

Ref. No:	263010921
From:	Public
Date:	01/09/21
Subject:	Ransomware incidents

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?

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?

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
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?

RESPONSE

We confirm that the Trust does hold the information that you have requested, however we are withholding this information under section 31 of the FOI Act.

Section 31(1)(a) provides an exemption from the right to know if disclosure would, or would be likely to, prejudice the prevention or detection of crime.

We consider listing detail on the payment of ransomware and technical details about the Trusts infrastructure would be likely to leave the Trust more vulnerable to targeted, malicious attacks on our systems. Hackers could use this information to their advantage to compromise our computer systems as such we consider withholding this information would be likely to prevent criminal activity.

We have considered the general public interest test in openness and transparency with regards to how public authorities use their resources However; we consider there is an overwhelming public interest in keeping the information held by the Trust (which includes patient identifiable data) within its computer systems secure.

We have therefore concluded the public interest is best served by withholding this information.