FREEDOM OF INFORMATION

FOI REFERENCE: 083/21	DATE RECEIVED: 31 August 21

REQUEST

I am writing to you under the Freedom of Information Act 2000 to request the following information from Staffordshire Fire and Rescue Service. Please can you answer the following questions:

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
    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?

RESPONSE

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
        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.) 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
        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/)?

        No

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

f. Had a formal policy on ransomware payment? No
   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? Yes
h. Paid consultancy fees for malware, ransomware, or system intrusion investigation No
   i. If yes at what cost in each year?
i. Used existing support contracts for malware, ransomware, or system intrusion investigation? No
j. Requested central government support for malware, ransomware, or system intrusion investigation? No
k. Paid for data recovery services? No
   i. If yes at what cost in each year?
l. Used existing contracts for data recovery services? No
m. Replaced IT infrastructure such as servers that have been compromised by malware? No
   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? No
   i. If yes at what cost in each year?
o. Lost data due to portable electronic devices being mislaid, lost or destroyed? No
   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?
   Not fully implemented yet
   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 Yes
   b. Desktop and laptop computers Yes
   c. Virtual desktops Yes
   d. Servers on premise Yes
   e. Co-located or hosted servers N/A
   f. Cloud hosted servers N/A
   g. Virtual machines Yes
   h. Data in SaaS applications N/A
   i. ERP / finance system N/A

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?
   Multiple systems are used
5. Do you have a cloud migration strategy? If so is there specific budget allocated to this?
   No
6. How many Software as a Services (SaaS) applications are in place within your organisation?
   4
   a. How many have been adopted since January 2020?
      0