GREATER**LONDON**AUTHORITY

[redacted]
(By email)

Our Ref: MGLA010921-1951

28 September 2021

Dear [redacted]

Thank you for your request for information which the Greater London Authority (GLA) received on 31 August 2021. Your request has been considered under the Freedom of Information Act 2000.

You requested:

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?*

Our response to your request is as follows:

The majority of this information is held by the GLA but is refused under section 31(1)(a) of the Act because its disclosure would be likely to prejudice the prevention or detection of crime.

The information in question would be likely to reveal details of the Authority's perceived strengths or weaknesses in relation to cyber security. As this is a qualified exemption, the Authority has considered whether, in all the circumstances of the case, the public interest in maintaining the exemptions outweighs the public interest in disclosing the information. The Authority acknowledges the general interest of the public in the Authority's cyber security processes. The importance of protecting the public and the Authority by maintaining the security of our information networks outweighs this interest in this case.

However, the GLA is able to respond to a number of your 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?) If yes, how many?*

    1 unsuccessful attempt

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

    No

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

    No

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

    Yes

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

    Yes

If you have any further questions relating to this matter, please contact me, quoting the reference MGLA010921-1951.

Yours sincerely

[redacted]
Information Governance Officer

If you are unhappy with the way the GLA has handled your request, you may complain using the GLA's FOI complaints and internal review procedure, available at:
https://www.london.gov.uk/about-us/governance-and-spending/sharing-our-information/freedom-information