

###  
###

###  
###  
Telephone: 0300 123 5500  
###

Date: 20 September 2021  
Our Reference: 12790541

Dear ###

### Information Request - 12790541 - ICT ransomware incidents etc

I am responding to your request for information, which has been considered under the Freedom of Information Act 2000 (FoIA) and logged as case 12790541.

Your request and response is as follows:

I confirm that Cheshire East Council holds the information you have requested. I have detailed below the information being released to you.

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?* **NCND**
  - b. *Had any data rendered permanently inaccessible by a ransomware incident (i.e. some data was not able to be restored from back up.)* **NCND**
  - 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.)* **NCND**
  - 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?* **NCND**
  - 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?* **NCND**
  - f. *Had a formal policy on ransomware payment?*
    - i. *If yes please provide, or link, to all versions relevant to the 3 year period.* **NCND**
  - g. *Held meetings where policy on paying ransomware was discussed?* **NCND**
  - h. *Paid consultancy fees for malware, ransomware, or system intrusion investigation*
    - i. *If yes at what cost in each year?* **NCND**

- i. *Used existing support contracts for malware, ransomware, or system intrusion investigation?* **NCND**
  - j. *Requested central government support for malware, ransomware, or system intrusion investigation?* **NCND**
  - k. *Paid for data recovery services?*
    - i. *If yes at what cost in each year?* **NCND**
  - l. *Used existing contracts for data recovery services?* **NCND**
  - m. *Replaced IT infrastructure such as servers that have been compromised by malware?*
    - i. *If yes at what cost in each year?* **NCND**
  - 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?* **NCND**
  - o. *Lost data due to portable electronic devices being mislaid, lost or destroyed?*
    - i. *If yes how many incidents in each year* **None**
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?* **NCND**
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.)* **NCND**
- 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?* **NCND**
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?*
- a. *How many have been adopted since January 2020?*
- We have approximately 28 SaaS applications in use, of which three have been added since January 2020. It is difficult to be definitive because of the subtle differences between SaaS and Vendor hosted solutions.**

The information requested is exempt from disclosure under Section 31(1) of the Freedom of Information Act (FoIA). Disclosure of this information would be likely to prejudice:

- a. the prevention or detection of crime,

To use this exemption we are required to undertake a public interest test. The matters which were considered in applying the public interest test are as follows:

Factors in favour of disclosure Cheshire East Council wishes to be as open as possible with the general public and to disclose as much information as is possible

Factors in favour of withholding in this case the information being requested will enable someone to determine the effectiveness of Cheshire East Council's ability to detect cyber attacks. This could compromise the authority's measures to protect its ICT systems. This would leave the authority vulnerable to future attacks.

It is considered that the greater public interest therefore lies in not providing the information at this time. In coming to that conclusion, the public interest in providing the information has been carefully weighed against any prejudice to the public interest that might arise from withholding the information; in all the circumstances of the case, the public interest in maintaining the exemption outweighs the public interest in disclosing the information.

This response therefore acts as a refusal notice under section 17 of the FoIA.

Please quote the reference number 12790541 in any future communications.

Please note that an anonymised copy of this response may be published in the Council's Disclosure Log, which is available online at the following address: [www.cheshireeast.gov.uk/foi](http://www.cheshireeast.gov.uk/foi)

If you are not satisfied with the outcome of your request or if you are not happy with the way your request has been handled, you can request an internal review. Internal review requests should be submitted within 20 working days of our response by emailing [foi@cheshireeast.gov.uk](mailto:foi@cheshireeast.gov.uk) or in writing to Compliance & Customer Relations Team, Cheshire East Council, 1st Floor, Westfields, c/o Municipal Buildings, Earle Street, Crewe, CW1 2BJ.

If you are not content with the outcome of the internal review, you then have the right to apply directly to the Information Commissioner for a decision. The Information Commissioner can be contacted at Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF; Tel: 0303 123 1113; Fax: 01625 524510 or <https://ico.org.uk> The Information Commissioner will not normally investigate your case until the Council's internal review process has been completed.

###  
###  
###