Information Governance Team

Postal Address:
Coventry City Council
PO Box 15
Council House
Coventry
CV1 5RR

www.coventry.gov.uk
E-mail: infogov@coventry.gov.uk
Phone: 024 7697 5408

20 July 2022

Dear Sir/Madam

Freedom of Information Act 2000 (FOIA)
Request ID: FOI431209691

Thank you for your request for information relating to council cyber-attacks.

You have requested the following information:

Q1. How many times has your council experienced an attempted cyber-attack over each of the past five years? For this and all relevant questions below, please provide data broken down into calendar year including 2022 to date, or failing that, by relevant 12-month period (e.g. 2020/21, 2021/22 etc.)
· 2022
· 2021
· 2020
· 2019
· 2018
See response below.

Q2. Of these attacks, how many resulted in the criminal being able to obtain data or disable systems?
· 2022
· 2021
· 2020
· 2019
· 2018
See response below.

Q3. Thinking about cyber-attacks where the criminal was able to obtain data or disable systems, how much have these cost your council in each of the past five years? If possible, please include the sum total of monies lost to hackers, legal costs and GDPR fines.
· **2022**
· **2021**
· **2020**
· **2019**
· **2018**
See response below.

Q4. What is the most common type of cyber-attack your council has experienced in 2022 so far? (e.g. phishing, DDoS, ransomware, password attack, malware, insider attacks)
See response below.

Q5. In the last 12 months have you employed an external expert to give you advice on how to mitigate the risk of cyber-attacks? If you have but not in the last 12 months please state when.

No.

Q6. Does your council currently hold a cyber-insurance policy to protect against the consequences of a cyber-attack?
See response below.

Q7. If so, have you claimed on this policy?
See response below.

Q8. Have you increased cyber security in the last year to mitigate the risk of cyber-attacks?

In response to Questions 1, 2, 3, 4, 6, 7 and 8 the Council under Section 31(3) neither confirms nor denies whether the information you have requested exists or is held by us.

The information you have requested is exempt from disclosure under Section 31(1)(a) and Section 31 (3) of the FOIA Act 2000. Section 31 of the FOIA relates to Law Enforcement and Section 31(3) removes the public authority's duty to confirm or deny whether information is held if to do so would, or would be likely to prejudice law enforcement.

It is the Council's view that the confirmation or denial of the possession of information relating to the Council's cyber resilience, would be likely to compromise the Council's information security strategies by giving cyber criminals insight into vulnerabilities which may, or may not, exist.

Section 31(3) is a qualified exemption, as such we have gone on to perform a public interest test in order to assess the public interest arguments for and against declaring whether or not the requested information is held.

For Disclosure:

• Confirmation of possession would demonstrate a commitment to transparency with regard to the Council's undertaking and could provide assurance that the council have robust IT infrastructure in place.

Against Disclosure:

• Maintaining the integrity and security of the Council's systems.
• Preventing cyber-attacks and similar against the Council systems.

Revealing the information may assist cyber criminal's insight into not only the strengths of the Council's cyber security, but also any potential weaknesses that may exist. This could ultimately result in a future cyber-attack. Cyber security measures are in place to protect the integrity of personal and sensitive personal information.

The occurrence of a future cyber-attack would prejudice the Council's legal duty to safeguard personal information from loss, theft, inappropriate access or destruction, which is why Section 31 has been employed in this case.

On balance the public interest in maintaining the exemption outweighs that in confirming or denying whether information is held and therefore the Council neither confirms nor denies, whether this information is held.

Q9. When did your council last hold training for employees aimed at reducing the role of human error in cyber-attacks and data breaches, e.g. to prevent phishing?

Council employees must undertake compulsory Annual Data Protection training which includes information/cyber security awareness.

Q10. Where on your corporate risk register is cyber risk ranked?
· **We don't have a risk register**
· **It is not on our risk register**
· **Outside of the top 10**
· **Three – ten**
· **Top three**

It is ranked on the risk register in the "three to ten" category.

The supply of information in response to a FOI/EIR request does not confer an automatic right to re-use the information. You can use any information supplied for the purposes of private study and non-commercial research without requiring further permission. Similarly, information supplied can also be re-used for the purposes of news reporting. An exception to this is photographs. Please contact us if you wish to use the information for any other purpose.

For information, we publish a variety of information such as: FOI/EIR Disclosure Log, Publication Scheme, Facts about Coventry and Open Data that you may find of useful if you are looking for information in the future.

If you are unhappy with the handling of your request, you can ask us to review our response. Requests for reviews should be submitted within 40 days of the date of receipt of our response to your original request – email: infogov@coventry.gov.uk

If you are unhappy with the outcome of our review, you can write to the Information Commissioner, who can be contacted at: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF or email icocasework@ico.org.uk.

Please remember to quote the reference number above in your response.

Yours faithfully

Information Governance