37666

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.)

This information is not recorded.

The nature of the world is that there can be many hundreds or even thousands of attempted breaches every day against a website or network. They will range from an individual trying to guess a password through to a "robot" scanning our defences looking for vulnerabilities to exploit. We build our system with protection mechanisms to stop the vast majority automatically, without logging them.

The Council is subject to an unquantifiable number of attempted Cyber Attacks on a daily basis, our Defence In Depth (DiD) approach to Cyber Security repels such attacks.

Of these attacks, how many resulted in the criminal being able to obtain data or disable systems?

None

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.

NA

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)

Does your council currently hold a cyber-insurance policy to protect against the consequences of a cyber-attack?

If so, have you claimed on this policy?

We will not provide this information.

In line with advice from the National Cyber Security Centre, we do not provide information relating to hardware, software and systems and therefore, unfortunately, it is not possible to provide you with the information you have requested on this occasion.

By placing information about our systems into the public domain we would potentially be putting our IT framework at risk. This would prejudice substantially the Council's ability to effectively carry out its business if its IT framework were compromised as a consequence of the disclosure of this information.

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

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

We have a fully outsourced ICT provision including Cyber Security.

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?

The Council sends out Monthly Awareness Training to all its employees who have access to its network.

Where on your corporate risk register is cyber risk ranked?

Cyber risk is included in the 'technology and information risk' included in the Corporate Leadership Team Risk Report presented quarterly to the Governance, Risk and Best Value Committee, and is ranked between three and ten.

The latest published risk report can be found at the following link:
https://democracy.edinburgh.gov.uk/documents/s43205/8.7%20-%20Corporate%20Leadership%20Team%20Risk%20Report%20as%20at%2024%20January%202022.pdf