Request 11270 - Council cyber-attacks

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

Q2 Of these attacks, how many resulted in the criminal being able to obtain data or disable systems?

· 2022
· 2021
· 2020
· 2019
· 2018

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

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)

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.

Q6. Does your council currently hold a cyber-insurance policy to protect against the

consequences of a cyber-attack?

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

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

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?

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

Response

Thank you for your request for information above, which we have dealt with under the terms of the Freedom of Information Act 2000.

I hope the following will answer your query:

Thank you for your information request above, which we have dealt with under the terms of the Freedom of Information Act (FOIA). We can confirm that we do hold information relevant to your request, however, we do find that some exemptions do apply and that some of your queries appear to be commercially orientated and we have grouped our responses together below:

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

Please find attached copy of the current strategic risk register.

The Freedom of Information Act exists to allow access to publicly held information, to promote open, accountable local government and to develop increased trust in government by ensuring transparent ways of working. However, information requests should be clearly within the wider public interest and where this wider public interest is not clear or where the request is of a commercial nature, the council may consider the request vexatious, which means we are not obliged to respond.

http://www.bailii.org/uk/cases/UKUT/AAC/2013/440.html

In this judgement Judge Wikeley indicates in paragraphs 35 and 38 that improper use of FOI [such as no public interest] is a valid consideration to make when considering if a request is vexatious. Using the Freedom of Information Act to gain a commercial advantage or seek opportunity over another can be included within this definition. It would be considered an abuse of a statutory process that is designed to promote open accountable local government, not provide commercial organisations with leads into organisations to promote or sell goods or services

Of course, a public body is not always aware of some wider public interests in a particular area, and we would like to seek clarification to be able to fully assess any possible public interest before fully considering your request.

You are invited to respond to assist our assessment of your request regarding your following questions:

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.

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

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

We consider the following questions to be exempt under s31(1)(a) – law enforcement, the prevention and detection of crime

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

Q2 Of these attacks, how many resulted in the criminal being able to obtain data or disable systems?

· 2022
· 2021
· 2020
· 2019
· 2018

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

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)

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

In relation to the application of s31(1) regarding requests for technical system information the Information Commissioners Office (ICO) advises:

Section 31 can be claimed by any public authority, not just those with law enforcement functions. · For example, section 31(1)(a) – prevention or detection of crime, can protect information on a public authority's systems which would make it more vulnerable to crime. It can also be used by a public authority that has no law enforcement function to protect the work of one that does. Please also see bullet point 5 of part 2. law-enforcement-foi-section-31.pdf (ico.org.uk)

Any disclosure made under the Freedom of Information Act, must be considered to be to the public at large, there is a real risk that this information could be used for criminal activity and the disclosure of this information increases that risk of prejudice to the prevention of crime.

Disclosure of such detail would be a security risk to the organisation. Section 31(1) is a qualified exemption which means a public interest test must be applied to see whether it is reasonable to disclose some or all of the information into the public domain. It would not be in the public interest to place material into the wider public domain that could be used to interfere with and place the organisation, its functions and its staff at risk of criminal activity, including theft and cybercrime. Therefore we decline to provide this information to you

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?

In response to this question, we are able to advise you of the following - All staff undergo induction training on key topics and various subjects relevant to their role, including aspects of IT and data management where required. Once this is complete staff will undertake annual refreshers in line with their role and personal development requirements. Induction and refreshers run on a rolling programme and are constantly available to staff.

We aim to provide a high-quality service to you and hope that you are satisfied with this response. If you have any further questions, please do not hesitate to contact us.