London Borough of Barnet,
2 Bristol Avenue, Colindale,
London NW9 4EW
21 June 2022
Our ref: 8316919

Thank you for your request received on 21 June 2022, for 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
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

We have processed this request under the Freedom of Information Act 2000.

Response

I can confirm that London Borough of Barnet holds the information you requested.

However, we believe that the exemptions detailed below apply to all of this information and this is withheld. Please see the Refusal Notice below.

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
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

S31 - Law Enforcement

This information is exempt from disclosure under Section 31(3) of the Freedom of Information 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.

Although the bona fides of the requester may be genuine FOI responses are public information and are made to the world. 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.

In applying this exemption, we have had to balance the public interest in withholding the information against the interest in favour of disclosure.

Factors in favour of disclosure

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

Factors in favour of withholding

* Maintaining the integrity and security of the council's systems
* Preventing cyber-attacks and similar against the council systems.
* Revealing whether or not the information requested is held or applicable to the London Borough of Barnet would be likely to offer cyber criminals 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. personal and

sensitive personal information.
* It is clear to see how 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.
* A cyber attack could have catastrophic consequences for council services for residents

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. In all the circumstances of the case, the public interest in maintaining the exemption outweighs the public interest in disclosing the information.

Further information

If you are interested in the data that the council holds you may wish to visit Open Barnet, the council's data portal. This brings together all our published datasets and other information of interest on one searchable database for anyone, anywhere to access. http://open.barnet.gov.uk/

Advice and Assistance : Direct Marketing

If you are a company that intends to use the names and contact details of council officers (or other officers) provided in this response for direct marketing, you need to be registered with the Information Commissioner to process personal data for this purpose. You must also check that the individual (whom you wish to contact for direct marketing purposes) is not registered with one of the Preference Services to prevent Direct Marketing. If they are you must adhere to this preference.

You must also ensure you comply with the Privacy Electronic and Communications Regulations (PECR). For more information follow this Link www.ico.org.uk

For the avoidance of doubt the provision of council (and other) officer names and contact details under FOI does not give consent to receive direct marketing via any media and expressly does not constitute a 'soft opt-in' under PECR.

Your rights

If you are unhappy with the way your request for information has been handled, you can request a review within the next 40 working days by writing to the Information Management Team at: foi@barnet.gov.uk. Or by post to Records & Information Management Service, Assurance Group, London Borough of Barnet, 2 Bristol Avenue, Colindale, NW9 4EW

If, having exhausted our review procedure, you remain dissatisfied with the handling of your request or complaint, you will have a right to appeal to the Information Commissioner at: The Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF (telephone: 0303 123 1113; website www.ico.org.uk). There is no charge for making an appeal.