2 Bristol Avenue,
Colindale, NW9 4EW
27 January 2021
Our ref: 6913616

Thank you for your request received on 7 January 2021, for the following information:
Council name

Region - please select from the following: South East, London, North West, East of England, West Midlands, South West, Yorkshire and the Humber, East Midlands, North East, Wales, Scotland, Northern Ireland

The total number of full-time and part-time employees employed by your organisation (as of 1st January 2021 or latest figures available)

The total number of full-time and part-time employees employed by your organisation with professional data security / cybersecurity qualifications (as of 1st January 2021 or latest figures available) - Common qualifications may include any cyber or IT security related qualifications such as CISSP, SSCP, CSA, CEH, CISA, CISM, Security+

The total number of full-time and part-time employees employed by your organisation who have completed cyber security training between 1stJanuary 2020 and 31stDecember 2020 (or latest annual figures available)

How much money (in pounds sterling) has been spent on cyber security training between 1stJanuary 2020 and 31stDecember 2020 (or latest annual figures available) this may include GDPR-related training

How many data breaches did your organisation report to the ICO between 1st January 2019 and 1st January 2020

How many data breaches did your organisation report to the ICO between 1st January 2020 and 1st January 2021

Was your organisation victim to a successful ransomware attack between 1st January 2020 and 31st December 2020? As for the definition of a 'successful ransomware attack', please include any incident in which an attacker requesting a ransom/payment managed to successfully encrypt, steal or leak any data/systems/assets that your organisation processes/holds.

If you answered yes to the previous question, did your organisation agree to pay a ransom? Yes/No

Did your organisation suffer a cyber security incident between 1st January

2020 and 31st December 2020 which resulted in disruption to the council's services? This refers to any cyber incident that forced usual services to go offline or become unavailable. Yes/No

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 consider that the following exemptionsapply to some of the information requested. The remaining information is not withheld and is below.

Council name

London Borough of Barnet

Region - please select from the following: South East, London, North West, East of England, West Midlands, South West, Yorkshire and the Humber, East Midlands, North East, Wales, Scotland, Northern Ireland

London

The total number of full-time and part-time employees employed by your organisation (as of 1st January 2021 or latest figures available)

Headcount 1654

Headcount FTE 1588.9.

The total number of full-time and part-time employees employed by your organisation with professional data security / cybersecurity qualifications (as of 1st January 2021 or latest figures available) - Common qualifications may include any cyber or IT security related qualifications such as CISSP, SSCP, CSA, CEH, CISA, CISM, Security+

LBB's IT is run by Capita PLC https://open.barnet.gov.uk/dataset/23d3v/customer-and-support-group-csg-contract + https://datapress-files.ams3.digitaloceanspaces.com/barnet/dataset/customer-and-support-group-csg-contract/2019-03-27T14%3A44%3A11/Information_Systems_Output_Specification__Final_for_Contract_Close__080413.pdf?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=PGFSIURNB2RGEURH2EBZ%2F20210127%2Fams3%2Fs3%2Faws4_request&X-Amz-Date=20210127T160723Z&X-Amz-Expires=300&X-Amz-Signature=7bf2e58c223d13f31b9eb47f3ce2f2902831dca8aff79ca87fff8cab367a4348&X-Amz-SignedHeaders=host and therefore this information is not held by the Council.

The total number of full-time and part-time employees employed by your organisation who have completed cyber security training between 1stJanuary 2020 and 31stDecember 2020 (or latest annual figures available)

Cyber Security is incorporated within our GDPR Training Module. As of September 2020, 90% of staff had completed this module.

How much money (in pounds sterling) has been spent on cyber security training between 1stJanuary 2020 and 31stDecember 2020 (or latest annual figures available) this may include GDPR-related training

This data is not availaible. We have a corporate e-learning system that contains mandatory modules to officers but individuals can attend additional training outside of corporate offering if their role requires it. In addition, this information is limited as LBB's IT is run by Capita PLC https://open.barnet.gov.uk/dataset/23d3v/customer-and-support-group-csg-contract + https://datapress-files.ams3.digitaloceanspaces.com/barnet/dataset/customer-and-support-group-csg-contract/2019-03-27T14%3A44%3A11/Information_Systems_Output_Specification__Final_for_Contract_Close__080413.pdf?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=PGFSIURNB2RGEURH2EBZ%2F20210127%2Fams3%2Fs3%2Faws4_request&X-Amz-Date=20210127T160723Z&X-Amz-Expires=300&X-Amz-Signature=7bf2e58c223d13f31b9eb47f3ce2f2902831dca8aff79ca87fff8cab367a4348&X-Amz-SignedHeaders=host and therefore some information is not held by the Council.

How many data breaches did your organisation report to the ICO between 1st January 2019 and 1st January 2020

7

How many data breaches did your organisation report to the ICO between 1st January 2020 and 1st January 2021

2

Was your organisation victim to a successful ransomware attack between 1st January 2020 and 31st December 2020? As for the definition of a 'successful ransomware attack', please include any incident in which an attacker requesting a ransom/payment managed to successfully encrypt, steal or leak any data/systems/assets that your organisation processes/holds.

We consider that the qualified exemption set out in Section 31 (Law enforcement) subsection (1)(a) applies to the information requested. Therefore, we have decided to withhold the information. Please see refusal notice below.

If you answered yes to the previous question, did your organisation agree to pay a ransom? Yes/No

N/A

Did your organisation suffer a cyber security incident between 1st January 2020 and 31st December 2020 which resulted in disruption to the council's services? This refers to any cyber incident that forced usual services to go offline or become unavailable. Yes/No

We consider that the qualified exemption set out in Section 31 (Law enforcement) subsection (1)(a) applies to the information requested. Therefore, we have decided to withhold the information. Please see refusal notice below.

Refusal Notice

We consider that the qualified exemption set out in Section 31 (Law enforcement) subsection (1)(a) applies to the information requested. Therefore, we have decided to withhold the information.
The information withheld is exempt under section 31 (1) (a). The Act states that the information will be exempt "if its disclosure under this Act would, or would be likely to, prejudice - (a) the prevention or detection of crime"

We consider that knowledge of the council's IS security provision would allow hackers or others with nefarious intent a head start in illegally accessing the council's systems. We also consider that disclosure of the requested information would increase the chances of a successful cyber-attack or similar on the council network or systems. Whilst no illegal intent is imported upon the requesters, a response provided to one legitimate requester under the Act is considered to be disclosure to the whole world. We consider 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

• Openness and transparency

• Knowledge that the council has appropriate security of its information and systems

Factors in favour of withholding

• Maintaining the integrity and security of the council's systems

• Maintaining the integrity and security of the council's data which includes large volumes of commercially sensitive, personal and sensitive personal data relating to staff and residents

• Preventing cyber-attacks and similar against the council systems.

• We consider that in all the circumstances of the case, the public interest in maintaining the exemption outweighs the public interest in disclosing the information.

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

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 Information Management Team (FOI) 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.