Request 8438 – Council data security

Under the Freedom of Information Act, I would like to ask for information on South Cambridgeshire's data security spending & training on behalf of Redscan.

Please could you share the following information in the format of an CSV, XLS, XLXF file - or any other format that may be opened via Excel or Google Spreadsheets (preferably not a pdf). If you wish to add more context or information, please do so in a separate document or in the body of an email.

N.B we intend on anonymising the results of this FOI when publishing it on the Redscan site. We do not wish to highlight which councils are performing better/worse than others (which would be irresponsible), we simply want to understand the risks posed to councils and how they approach training/qualifications.

1) Council name:

2) 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:

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

4) 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+:

5) 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):

6) 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:

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

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

9) 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.:

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

11) 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:

Response

1) Council name: South Cambridgeshire District Council

2) 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: East of England

3) The total number of full-time and part-time employees employed by your organisation (as of 1st January 2021 or latest figures available): 604

4) 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+: Unknown – IT is outsourced

5) 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): None – IT is outsourced

6) 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: Nil

7) How many data breaches did your organisation report to the ICO between 1st January 2019 and 1st January 2020: - 0

8) How many data breaches did your organisation report to the ICO between 1st January 2020 and 1st January 2021: - 0

9) 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.: No

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

11) 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: No