Our Reference: 2423

FOI Request dated 04/07/2021 as follows –

I wish to submit a formal request for information under the Freedom of Information Act. If you do not hold data on one of the questions or if it could be rejected based on time constraints, please feel free to leave this answer out. If colleagues have enough time to also provide some comments and/or reasoning for their answers, I would be most grateful.

1. What is the total number of cyber security and data breaches, if any, reported to the Information Commissioner's Office within the last 12 months.

2. What is the approximate number of phishing and spam emails the university has been sent in the past 12 months?

3. Does the university hold a NCSC Cyber Essentials certificate?

4. What is the total number of staff with a cyber-security and/or data security qualification.

5. What is the frequency, if any, of penetration testing the university has contracted/carried out within the last 12 months.

6. What is the approximate total amount of money spent on staff's cyber security training in the last 12 months.

7. What is the percentage of all staff who have completed basic cyber security training (such as, a brief online course, qualification or awareness day training).

Response

Please note the last 12 months form date of your request and figure as of September 2021.

1. What is the total number of cyber security and data breaches, if any, reported to the Information Commissioner's Office within the last 12 months. **– Total 3 (as of September 2021)**

2. What is the approximate number of phishing and spam emails the university has been sent in the past 12 months? **Approximately 460,000 per month equating to 5.52 million over the last 12 months**

3. Does the university hold a NCSC Cyber Essentials certificate? **- Section 1 of the Freedom of Information Act 2000 (FOIA) places two duties on public authorities. Unless exemptions apply, the first duty at Section 1(1)(a) is to confirm or deny whether the information specified in a request is held. The second duty at Section 1(1)(b) is to disclose information that has been confirmed as being held. Where exemptions are relied upon Section 17 of FOIA requires that we provide the applicant with a notice which: a) states that fact b) specifies the exemption(s) in question and c) states (if that would not otherwise be apparent) why the exemption applies. It has been determined that this information is exempt on the basis that s21 of the Act applies – Information Reasonably Accessible by Other Means. As this exemption is absolute there is no requirement for me to conduct a public interest test, however in order to provide assistance I provide the following link - Verify suppliers - NCSC.GOV.UK**

4. What is the total number of staff with a cyber-security and/or data security qualification. **– 4 Members within the ICT Department**

5. What is the frequency, if any, of penetration testing the university has contracted/carried out within the last 12 months. **– We are unable to provide the requested information on this occasion, in line with Section 17 of the Act, this response acts as a Refusal Notice. The Act contains a number of exemptions that allow public authorities to withhold certain information from release. We have applied the following exemption to your request – Section 31 (1)(a) – Law Enforcement.**

As with other large organisations; universities are reliant on the smooth running of their IT Networks. Maintaining the security of these networks is a significant challenge for all universities, who are increasingly subject to both general cyber security threats and targeted attempts to obtain information from students/staff. Release of any information under the Act represents a disclosure to the word, and it is our belief that if information was disclosed about the frequency of penetration testing the university has contracted or carried out within the last 12 months, a m0otivated individual or group could use this information to target any potential vulnerabilities, exposing the University's IT systems to various types of unlawful attack, and consequently prejudicing the prevention of criminal activity.

Having determined the aforementioned in that disclosure of this information would expose the University to a real and significant risk of crime, application of S31 (1) Law Enforcement also requires us to consider the public interest in withholding/disclosing the information.

Factors in favour of disclosure –

- **Increase public understanding of the University's information technology systems and processes, and how it manages its business.**
- **Enhancing the transparency and accountability of our cyber security system and about our ability to protect our systems and assets.**

Factors against disclosure –

- **Protecting the ability of public authorities to protect valuable public assets acquired with public funds.**
- **There is a strong public interest in not publishing information which might expose the University to cyber-attacks and in preventing criminal activity that could damage the running of the University and the security aspect of the information held.**

  After considering the above factors, we believe the factors against disclosure outweigh those in favour, and therefore applying Section 31 on this basis.

6. What is the approximate total amount of money spent on staff's cyber security training in the last 12 months. **- ICT do not have a dedicated info-sec training budget but a general ICT training budget of £32K**

7. What is the percentage of all staff who have completed basic cyber security training (such as, a brief online course, qualification or awareness day training). **– Information not held**.