FOI Request dated 12/02/2024

Request Reference: 3072

Please find below my FOI request regarding ransomware attacks on the college/university.

1. In the last 5 years, how many times has your college/university suffered from a ransomware attack? Please provide specific dates (months/years) if possible.
2. How much downtime did this cause (in hours)?
3. Did you pay the ransom? If so, how much was the ransom?
4. What type of ransomware was used?
5. What was the total cost of the incident to your college/university?
6. How many student and/or staff records were impacted in the breach?

If you don't have data available for all of the questions, please provide any data you do have.

Response

University of Hull can neither confirm nor deny it holds any information with regards to an exempt body as the duty in Section 1 (1)(a) of the Freedom of Information Act 2000 does not apply by virtue of the following exemption:

- Section 31 (3) Prevention and Detection of Crime

Section 31(3) sets out that information is exempt from disclosure as its release would or would be likely to prejudice the prevention or detection of crime. To confirm nor deny information regarding the number and dates of ransomware attacks would provide attempted attackers with information regarding our cyber-defence provision. It would indicate whether attempts have been detected and/or successful. This information could be used by motivated individuals in order to target the University, or to adapt behaviour in order to avoid detection.

Section 31(3) is a qualified exemption. This means that the University of Hull is required to consider whether the public interest in the information outweighs the public interest in maintaining the exemption.

There is clearly a very strong public interest in protecting public authorities from crime. To confirm nor deny such information increases the University's vulnerability to cyber-crime and would jeopardise our ability to provide services to our students (current, former and potential), and would put at risk personal, financial and commercial sensitive information. We therefore consider that there is a very strong public interest in maintaining the exemption.

Conversely, we do not consider there to be any particular public interest in confirming nor denying this information. While it is important for students and the public to understand that the University takes the

threat of cyber-crime seriously, and are taking appropriate measures to tackle it, we do not consider that this interest would be furthered by confirming or denying any information. We therefore consider that the public interest is firmly in favour of a neither confirm nor deny stance.