Freedom of Information Act 2000 - Request Reference FoI/23/510
Cybersecurity Budget

Information Requested:

1. In 2023, what annual cybersecurity budget has been allocated to your NHS Trust?

2. Can you also provide your Trust's annual cybersecurity budget for the years:
    a. 2022
    b. 2021
    c. 2020
    d. 2019
    e. 2018
    f. 2017

3. In 2023, how is your annual cybersecurity budget spent:
    a. What percentage goes towards cybersecurity training for employees?
    b. What percentage goes towards technology investments?
    c. What percentage goes towards employee resources for your cybersecurity team?

4. How many employees work in your NHS Trust?

5. How many employed, full-time members of staff make up your NHS Trust's cyber/infosecurity team?

6. How many hours of cybersecurity training are employees of your NHS Trust required to undertake every year?

7. Has your NHS Trust paid any ransom demands to cybercriminals in the last five years?
    a. If yes, how much did you pay in total?

8. Has your NHS Trust had any patient records compromised / stolen by cybercriminals in the last five years?
    a. If yes, how many records were compromised / stolen?

Response Details:

Response to questions 1-3 and 5-8:

Cardiff and Vale University Health Board (the UHB) is withholding this information, relying on Section 31 (1) (a) of the Freedom of Information Act 2000 (prevention and detection of crime). Specifically, the UHB believes that disclosing details regarding its ICT infrastructure, or support of that infrastructure, would be likely to prejudice the prevention of crime, particularly cyber-crime. As this is a qualified exemption, the UHB is required to complete a public interest test in deciding whether it is in the public's interest to withhold or disclose the information.

Public Interest Test:

In favour of disclosure: The UHB recognises there is a public interest in transparency and in public authorities demonstrating that their systems effectively protect personal data.

Against disclosure: There is a very strong public interest in protecting the extremely sensitive data held by the UHB. Cyber Security and the associated Cyber-Risk / Cyber-Attacks represent a rapidly evolving arena that becomes more complex and dangerous with time. Releasing details of the UHB's ICT infrastructure (or the finances available to support it) into the public domain significantly reduces its capacity to manage this threat to the stated public interest by exposing potential vulnerabilities.

Decision: The UHB considers that the public interest in withholding the information is significantly greater than any interest there may be in disclosing it and potentially exposing sensitive personal data to an increased level of risk. The UHB strongly believes that posing additional unnecessary risk to the UHB, and consequently patient care and safety, would be viewed as an unacceptable risk by the public. Whilst the UHB acknowledges a public interest in providing assurances of effective protection of personal data, it believes the most effective means of increasing public confidence in data protection is to successfully protect the data itself. The UHB considers its responsibility to protect the personal data of patients and staff to be of the highest importance. It was therefore decided that it was not in the public's interest to disclose this information.

Response to question 4:

Cardiff and Vale University Health Board has 17,306 employees.