Reference:	FOI.12787.23
Subject:	Cyber security
Date of Request:	2 October 2023

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:

Hywel Dda University Health Board (UHB) is unable to provide the information requested for questions 1 - 3 and 5 - 8, as it has deemed that the information is exempt from disclosure under Section 31(1)(a) of the Freedom of Information Act 2000 (FoIA). The UHB has also considered the "mosaic effect"; the harm which will or will be likely to arise from the release of this information along with information already in the public domain.

Section 31(1)(a) of the FoIA provides that information which is not exempt by virtue of Section 30 (criminal investigations and proceedings) is exempt if its disclosure would, or would be likely to, prejudice the prevention or detection of crime. The Information Commissioner's Office (ICO) guidance advises that Section 31, amongst other things, prevents information being disclosed that would increase the risk of the law being broken. In addition, it can be claimed by any public authority. The UHB is relying upon this exemption as it considers that releasing this information about our IT systems would, in the present climate, make it more vulnerable to crime.

Section 31(3) of the FoIA provides that the duty to confirm or deny does not arise in relation to this information.

Section 31 of the FoIA is subject to the public interest test.

In favour of disclosure: The UHB has a duty to maintain openness and transparency in all its activities, which will help to maintain public trust in the UHB.

In favour of non-disclosure: By releasing the information, the UHB would be vulnerable to this being used for crime, which potentially could compromise the security of both patient and staff information, whilst causing disruption to the flow of information through the UHB systems, impacting on patient care and safety. There is a clear public interest in protecting society and the UHB from the impact of crime. The UHB has given consideration to a cyber attack in the NHS, in recent years, which is already in the public domain.

Decision: The UHB considers that the public interest in withholding the information is greater than the interest in disclosing, therefore protecting the UHB from potential criminal activity.

4. The UHB can confirm that as of 30th September 2023, there were 14,079 people employed in the Health Board.