Reference: FOI.ICB-2425/185

Subject: Cyber Security Incidents and Training

I can confirm that the ICB does hold some of the information requested; please see responses below:

QUESTION	RESPONSE
1. How many cyber incidents occurred in the last two years (1st of July 2022-1st of July 2024)? Please provide separate information on: • Cyber incidents that occurred within the NHS Bristol, North Somerset and South Gloucestershire ICB • Cyber incidents NHS Bristol, North Somerset and South Gloucestershire ICB reported to NHS England	Zero
2. During the period from 1st of July 2022 -1st of July 2024, please provide accurate information on or the closest estimates for: • The number of rescheduled patient appointments due to cyber incidents • The number of incidents that were a result of human error • The duration of any system downtime caused by the incident • The number of data breaches that occurred • The number of patients affected by data breaches	The ICB does not hold this information. Any incidents relating to cyber breaches will be held by SCW CSU (South Central and West Commissioning Support Unit). Please contact NHS England: england.contactus@nhs.net https://www.england.nhs.uk/contact-us/foi/

3. What percentage of your organisation's total training budget is allocated to cybersecurity-related training for the current fiscal year? ___%	This fiscal year has not yet had any allocated funding. About 10.3% of FY-2023 was allocated to a comprehensive solution to begin in mid-late 2024. Nothing has yet been allocated toward cybersecurity specific funding for FY-24. This will be evaluated in Quarter 4 (Jan-Mar).
4. Does your organisation have a formal cybersecurity skills assessment process to identify skill gaps among employees? Yes / No If yes, please provide information on: A. A description of the assessment methodology B. The frequency with which these assessments are conducted C. How the results of these assessments inform training initiatives	No formal skills assessment has been implemented. We are beginning work with a cybersecurity training provider called SoSafe Gmbh beginning with a phishing simulation and personalised learning tracks for cybersecurity awareness and skills will be implemented. Previous phishing simulations by our IT team was the assessment process beforehand.
5. Has your organisation implemented specific measures to address and mitigate cybersecurity risks associated with human error? Yes / No If yes, please provide information on: A) Targeted training programmes B) Awareness campaigns C) Any technological solutions implemented to reduce the risk of human error	Yes, the ICB uses/has implemented the following: • Acceptable use of IT policies • Multi-Factor Authentication • Cloud Hosting • Microsoft Office 365

The information provided in this response is accurate as of 9 September 2024 and has been approved for release by Deborah El-Sayed, Chief Transformation and Digital Officer for NHS Bristol, North Somerset and South Gloucestershire ICB.