Reference: FOI.ICB-2425/164

Subject: Cyber Security

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

QUESTION	RESPONSE
1. How many cyber incidents (threat and breach) occurred in the last two years (1st of July 2022-1st of July 2024)?	Zero Major Cyber Incidents have occurred in the last two years.
2. For each of the following cyber incident types, please indicate if your organisation experienced them in any month from the 1st of July 2022- 1st of July 2024. If yes, specify the month(s) in which they occurred: i. Phishing attacks: Yes/No. If yes, which month(s)? ii. Ransomware attacks: Yes/No. If yes, which month(s)? iii. Distributed Denial of Service (DDoS) attacks: Yes/No. If yes, which month(s)? iv. Data breaches: Yes/No. If yes, which month(s)? v. Malware attacks: Yes/No. If yes, which month(s)? vi. Insider attacks: Yes/No. If yes, which month(s)? vii. Cloud security incidents: Yes/No. If yes, which month(s)? viii. Social engineering attacks (excluding phishing): Yes/No. If yes, which month(s)? ix. Zero-day exploits: Yes/No. If yes, which month(s)	No

3. For each of the following supplier types, please indicate if any cyber incidents related to them occurred between the 1st of July 2022-1st of July 2024. If yes, specify the volume of cyber incidents that occurred: i. IT service providers: Yes/No ii. Medical equipment suppliers: Yes/No iii. Software vendors: Yes/No iv. Cloud service providers: Yes/No v. Data storage/management companies: Yes/No vi. Telecommunications providers: Yes/No vii. Security service providers: Yes/No viii. Managed service providers (MSPs): Yes/No ix. Third-party payment processors: Yes/No	No
4. During the period from 1st of July 2022 -1st of July 2024, did your organisation experience any of the following impacts due to cyber incidents? i. Were any appointments rescheduled due to cyber incidents? Yes/No ii. Was there any system downtime lasting more than 1 hour? Yes/No iii. Did any data breaches occur? Yes/No iv. Were any patients affected by data breaches? Yes/No	None.
5. What percentage of your cybersecurity budget is allocated to each of the following supply chain security technologies? Please indicate the percentage for each: i. Third-party risk assessment tools: ___% ii. Vendor management systems: ___%	The ICB does not currently have a specific budget for cyber security. We do use centrally funded cyber tools.

iii.	Supply chain visibility and monitoring solutions: ___%	
iv.	Secure data sharing platforms: ___%	
v.	Multi-factor authentication for supplier access: ___%	
vi.	Endpoint detection and response (EDR) for supplier systems: ___%	
vii.	API security solutions: ___%	

The information provided in this response is accurate as of 7 August 2024 and has been approved for release by Seb Habibi, Deputy Chief Transformation and Digital Officer for NHS Bristol, North Somerset and South Gloucestershire ICB.