Reference: FOI.ICB-2627/008

Subject: Cyber Security Breaches Data and Costs

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

QUESTION	RESPONSE
Under the Freedom of Information Act, I would like to request the following information for each calendar year from 2020 to 2026 inclusive:	
1. The number of cyber security breaches that have being identified that were found to be a result of a malicious threat actor (i.e. not accidental data breach)	The ICB has applied Section 24 (Safeguarding National Security) to questions 1, 2, 3 and 4 as disclosing the information would make local healthcare systems vulnerable to cyberattack. Section 24 is a qualified exemption and subject to the public interest test. This has been outlined below. Public Interest test for Section 24 application The ICB believes that disclosure of the requested information would leave local healthcare IT systems vulnerable to cyberattack. The exemption has been considered in more detail below: Public interest in disclosing the information The public interest arguments in favour of disclosing the information took into account the FOIA definition of where there is a public interest.
2. The breakdown in high-level causes of these breaches as identified by cyber security incident response teams (CSIRTs), for example (but not limited to) unpatched software/hardware, lack of multi-factor authentication (MFA), leaked user credentials, lack of in-transit encryption, etc	
3. The number of breaches that occurred that were attributed to a previously known vulnerability to the organisations hardware, software, policies, or processes, for example where system was known to be at risk due to being unpatched or out of support, or security controls were recommended but not enforced, and was defined within the resulting incident response report.	

4. The estimated combined costs incurred as a result of cyber security breaches defined in request number one in each year.	The ICB recognises that there is a public interest in the number of breaches and the cost incurred by a public authority as a result of these breaches. The ICB IT system holds data which supports the local population to receive health care services as well as highly sensitive, personal special category data and therefore there is a public interest in understanding how many cyberattacks have occurred. The ICB also recognises that there is a public interest in the cost resulting from any cyberattacks as the NHS is publicly funded. <u>Public interest argument in favour of maintaining the exemption</u> The ICB believes that by disclosing the number, the causes, any identified vulnerabilities and the cost (which may indicate the number) would make BNSSG ICB (and wider) systems more vulnerable to cyberattacks as targeted attacks could take place. Cyberattacks cannot be predicted but particularly within the NHS should be expected. Healthcare providers are a known target for cyberattacks due to the large amounts of confidential and personal data held and this data can be sold for significant amounts of money. Cyberattacks to these systems could result in data breaches, healthcare providers not having access to patient data or the systems required to provide care, and costs to the ICB related to emergency measures or equipment repairs. Patient health and care would be negatively affected if there was a successful attack on the ICB systems. The information requested would likely be of interest to those with malicious intent rather than the general public who would likely want assurances that the ICB was protecting the ICB against security threats.

	The GDPR requires organisations to process personal data securely and "…ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures." As part of this, organisations are expected to have measures in place to protect against cyberattack. Training has been provided to ICB staff which has alerted staff to possible disclosures which may be detrimental to cyber security. Disclosure of data relating to cyber security breaches has been identified as an area of risk. <u>Public Interest Test</u> Under the Network and Information Systems (NIS) regulations, ICBs are considered "operators of essential services" in the health sector. This means ICBs are responsible for ensuring the security of the network and information systems which support essential healthcare systems such as infrastructure for healthcare providers. The ICBs must take appropriate action to manage risk, prevent incidents and ensure service continuity. The ICB believes that applying Section 24 to the questions manages this risk appropriately in line with ICB responsibilities. The ICB has considered the public interest in the information and weighed the risk of cyberattacks against this. The ICB has applied a risk based approach to the application of Section 24 and considered: • the public interest in the safety of data held by the NHS • the public interest in the costs resulting from cyber security breaches • the interest of the public in the high level causes of the security breaches and the system vulnerabilities

	• the interest of those with malicious intent in the high level causes of the security breaches and the system vulnerabilities • the significant threat of cyberattack to the NHS • the legal requirements of the NHS to protect personal data under the Data Protection regulations • the requirements under NIS regulations to protect cyber security • the impact of a cyberattack (significant financial impact, loss of trust in services, personal impact for patients both in terms of care and associated with data breaches, impact on health and social care staff) • the wider impact on the health and social care system of a cyberattack In its consideration of the above points, the ICB has applied Section 24 as the public interest in the information does not outweigh the risks should a cyberattack occur due to the disclosure of the information. The public interest lies in maintaining continuity of services and ensuring that data remains secure.

The information provided in this response is accurate as of 22 April 2026 and has been approved for release by Seb Habibi, Interim Chief Transformation and Digital Information Officer for NHS Bristol, North Somerset and South Gloucestershire ICB.