

Ref. No: 1122
Date: 06/08/24
Subject: Interest in supply chain cybersecurity

REQUEST

1. How many cyber incidents ([threat](#) and [breach](#)) occurred in the last two years (1st of July 2022-1st of July 2024)?

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:

- Phishing attacks: Yes/No. If yes, which month(s)?
- Ransomware attacks: Yes/No. If yes, which month(s)?
- Distributed Denial of Service (DDoS) attacks: Yes/No. If yes, which month(s)?
- Data breaches: Yes/No. If yes, which month(s)?
- Malware attacks: Yes/No. If yes, which month(s)?
- Insider attacks: Yes/No. If yes, which month(s)?
- Cloud security incidents: Yes/No. If yes, which month(s)?
- Social engineering attacks (excluding phishing): Yes/No. If yes, which month(s)?
- Zero-day exploits: Yes/No. If yes, which month(s)?

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:

- IT service providers: Yes/No
- Medical equipment suppliers: Yes/No
- Software vendors: Yes/No
- Cloud service providers: Yes/No
- Data storage/management companies: Yes/No
- Telecommunications providers: Yes/No
- Security service providers: Yes/No
- Managed service providers (MSPs): Yes/No
- Third-party payment processors: Yes/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?

- Were any appointments rescheduled due to cyber incidents? Yes/No

- Was there any system downtime lasting more than 1 hour? Yes/No
- Did any data breaches occur? Yes/No
- Were any patients affected by data breaches? Yes/No

5. What percentage of your cybersecurity budget is allocated to each of the following supply chain security technologies? Please indicate the percentage for each:

- Third-party risk assessment tools: ___%
- Vendor management systems: ___%
- Supply chain visibility and monitoring solutions: ___%
- Secure data sharing platforms: ___%
- Multi-factor authentication for supplier access: ___%
- Endpoint detection and response (EDR) for supplier systems: ___%
- API security solutions: ___%

RESPONSE

St Helens and Knowsley Teaching Hospitals NHS Trust and Southport and Ormskirk Hospital NHS Trust became a single legal entity known as Mersey and West Lancashire Teaching Hospitals NHS Trust on 1st July 2023, as such parts of the response may be provided in two sections relating to the hospital sites of each of the legacy organisations.

The information is exempt from disclosure under the Freedom of Information Act.

Section 31(1)(a) of the Act states:

31. Law enforcement.

(1) Information which is not exempt information by virtue of section 30 is exempt information if its disclosure under this Act would, or would be likely to, prejudice—

(a) the prevention or detection of crime,

Guidance from the Information Commissioner's Office states:

Section 31(1)(a) will cover all aspects of the prevention and detection of crime...The exemption also covers information held by public authorities without any specific law enforcement responsibilities...It could also be used to withhold information that would make anyone, including the public authority itself, more vulnerable to crime for example, by disclosing its own security procedures.

Information disclosed under Freedom of Information becomes publicly available. This means that the impact of disclosure must be considered from

the general release of information and not limited to disclosure to one individual (the requestor).

The Trust determines that to disclose specific information regarding its cyber security protection and the outcome of any attack would prejudice the security of the systems by allowing for the assessment of the Trust's security procedures and where, if any, vulnerabilities exist. Consequently section 31 (1) (a) is being applied to this request.

The trust is also exempting part of this request under section 43.2

The Freedom of Information Act gives the public a general right of access to information held by a public authority, including activity and financial details, subject to exemptions within the Act.

Section 43 – Commercial Interests - sets out an exemption from the right to know if:

The release of the information is likely to prejudice the commercial Interests of any person. (A person may be an individual, a company, the public authority itself or any other legal entity.)

Information can only be withheld under this exemption if the public authority is satisfied that to release the information would damage someone's commercial Interests. A commercial Interest relates to a person's ability to participate competitively in a commercial activity

Where a public authority is satisfied that the release of information would prejudice someone's commercial Interests, it can only refuse to provide the information if it is satisfied that the public Interest in withholding the information outweighs the public Interest in disclosing it.

The bias is in favour of disclosure and there will be occasions where information is released even though it is likely to prejudice someone's commercial Interest. If the public Interest is in favour of disclosure, the FOIA requires the information to be released.

The public interest test undertaken is specifically in relation to section 43(2) with the prejudice to commercial interests being those of the Trust (as the public authority).

Public Interest Arguments	
In favour of disclosure	In favour of non-disclosure
<ul style="list-style-type: none">• There is a general public Interest in the income, expenditure and activity of public authorities.• To increase the accountability of the public authority.• To increase the transparency of	<ul style="list-style-type: none">• A business case could be produced from the information based upon the service supply, demand and cost information.• The information could induce further competitors to the market.

<p>the public authority.</p> <ul style="list-style-type: none"> • Promote competition in the industry 	<ul style="list-style-type: none"> • Could prejudice SOH's negotiations with other organisations as it would be known what the demand and costs are of the service. • The information requested is for the current year therefore attracts significant time sensitivity. • It is not possible for the authority to gain the reciprocal information from private providers, giving the private providers an unfair advantage
--	--

Outcome In accordance with section 1 (1) the Freedom of Information Act, It can be confirmed that the information is held by the authority. In the balance of the public interest test under section 43 of the FOIA the Trust determines that the public Interest is in the non-disclosure of the information requested.

The Trust is aware that Cyber spend and incidents are of interest to the public.

The combination of this information could then allow a business case to be produced to directly compete with NHS service providers including Mersey and West Lancashire teaching Hospitals NHS Trust. Furthermore the Trust is of the opinion that the information is likely to be used for this purpose.

This would have an adverse impact of the commercial activity of the authority therefore section 43 (2) of the Freedom of Information Act is engaged.