Alder Hey Children's NHS
NHS Foundation Trust

Reference Number: FOIAH2425/226

From: Private Individual

Date: 24 July 2024

Subject: Cyber Security Incidents and Budget

Q1 How many cyber incidents (threat and breach) occurred in the last two years (1st of July 2022-1st of July 2024)?

A1 Regarding cyber threats, Information exempt under s31 – law enforcement, specifically section 31 (1) (a) relating to the prevention and detection of crime.

We have assessed the public interest in disclosure and believe the only factor for release would be openness and transparency, however the factors against release clearly outweigh this as release of the information would place the Trusts information systems and other related assets at risk of attack from hackers if released in to the public domain. This would have a major impact on the Trusts ability to maintain confidentiality, integrity and availability of systems and information and would severely disrupt services to our patients and would have a substantial impact on the Trusts reputation therefore causing financial loss and would damage the Trusts commercial interests.

Regarding cyber breaches, any reportable incidents would be published; therefore, this information exempt under Section 21 of the Freedom of Information Act 2000 - 'Information reasonably accessible to the applicant by other means'

Q2 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)

A2 Information exempt under s31 – law enforcement, specifically section 31 (1) (a) relating to the prevention and detection of crime.

We have assessed the public interest in disclosure and believe the only factor for release would be openness and transparency, however the factors against release clearly outweigh this as release of the information would place the Trusts information systems and other related assets at risk of attack from hackers if released in to the public domain. This would have a major impact on the Trusts ability to maintain confidentiality, integrity and availability of systems and information and would severely disrupt services to our patients and would have a substantial impact on the Trusts reputation therefore causing financial loss and would damage the Trusts commercial interests.

Q3 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

A3 Information exempt under s31 – law enforcement, specifically section 31 (1) (a) relating to the prevention and detection of crime.

We have assessed the public interest in disclosure and believe the only factor for release would be openness and transparency, however the factors against release clearly outweigh this as release of the information would place the Trusts information systems and other related assets at risk of attack from hackers if released in to the public domain. This would have a major impact on the Trusts ability to maintain confidentiality, integrity and availability of systems and information and would severely disrupt services to our patients and would have a substantial impact on the Trusts reputation therefore causing financial loss and would damage the Trusts commercial interests.

Q4 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

A4 Information exempt under s31 – law enforcement, specifically section 31 (1) (a) relating to the prevention and detection of crime.

We have assessed the public interest in disclosure and believe the only factor for release would be openness and transparency, however the factors against release clearly outweigh this as release of the information would place the Trusts information systems and other related assets at risk of attack from hackers if released in to the public domain. This would have a major impact on the Trusts ability to maintain confidentiality, integrity and availability of systems and information and would severely disrupt services to our patients and would have a substantial impact on the Trusts reputation therefore causing financial loss and would damage the Trusts commercial interests.

Regarding data breaches, any reportable breaches would be published; therefore this information is also exempt under Section 21 of the Freedom of Information Act 2000 - 'Information reasonably accessible to the applicant by other means'.

Q5 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: ___%

A5 Information not held, the Trust does not specifically record % of budget allocated to each element.