Liverpool Heart and Chest Hospital NHS
NHS Foundation Trust

Reference Number: FOI202223/373
From: Private Individual

Date: 04 January 2023

Subject: Outsourcing of teleradiology services

Q1 What was the total number of cyber attack incidents that have been recorded in your trust in the past 24 months?

A1 Information not held- While incidents are logged there is no separate category for cyber attack or similar to report on.

Q2 What is the classification of your policy regarding breach response?

A2 No specific breach policy.

Q3 Of the devices running Windows operating systems, what is the number and percentage of devices running Windows 11, Windows 10, Windows 7, Windows XP?

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

Whilst we can confirm we have some legacy windows installs in place the detail of such is exempted under Section 31 law enforcement, relating to the prevention and detection of crime.

We have assessed the public interest in disclosure and believe that whilst factors 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 into 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 What are the top 20 cyber security risks in your Trust, and how are they managed?

A4 Information exempt under Section 31 – law enforcement, specifically section 31 (1) (a) relating to the prevention and detection of crime, as per A3

Q5 Do you continue to use the Unified Cyber Risk Framework, is so how many risks are still identified/managed.

A5 We do not specifically use the Unified Cyber Risk Framework, however we do reference a number of good practice frameworks such as this to inform our control framework as well as maintain compliance to mandatory standards.

Q6 What is your Patch Management Cycle and how is it implemented on old Operating

systems (e.g., for Windows , Windows XP)?

A6 Information exempt under Section 31 – law enforcement, specifically section 31 (1) (a) relating to the prevention and detection of crime, as per A3

Q7 What is your current status on unpatched Operating Systems?

A7 Information exempt under Section 31 – law enforcement, specifically section 31 (1) (a) relating to the prevention and detection of crime, as per A3

Q8 Of the devices running Windows Servers operating systems, what is the number and percentage of devices running Windows 2000, Windows 2003, Windows 2008, Windows 2012, Windows 2016, Windows 2019, Windows 2022?

A8 Information exempt under Section 31 – law enforcement, specifically section 31 (1) (a) relating to the prevention and detection of crime, as per A3

Q9 Has your Trust signed up to and implemented the NHS Secure Boundary managed service to strengthen cyber resilience? If so, how many cyber security threats has the NHS Secure Boundary detected within your NHS Trust since its implementation?

A9 We have signed up to, and implemented, the NHS Secure Boundary managed service. However, we do not collate statistics on the alerting we have received from this channel.

Q10 Does your Trust hold a cyber insurance policy? If so:
a. What is the name of the provider;
b. How much does the service cost; and
c. By how much has the price of the service increased year-to-year over the last three years?

A10 We do not currently hold cyber insurance.

Q11 When did the current Board last receive a briefing on cybersecurity threats within healthcare, and when did they last participate in cyber security training? How frequently, if at all, do these briefings and trainings occur, and are they carried out by cyber security technology professionals?

A11 The Board receive monthly updates on our IT infrastructure via reporting from delegated subgroups. If a specific major threat is identified than a specific briefing would be produced.

Q12 Has your NHS Trust completed a Connection Agreement to use the Health and Social Care Network (HSCN)? If so, did you pass, and is there a copy of the code of connection?

A12 There is a connection agreement, and it is no longer a pass or fail as such, it is compliant with Data Security and Protection Toolkit (DSPT) annually, which we do meet and there is a register of those organisations on the DSPT website - https://www.dsptoolkit.nhs.uk/OrganisationSearch

Q13 Have there been any incidents of staff members or personnel within your Trust being let go due to issues surrounding cyber security governance?

A13 Information not held – No incidents

Q14 How many open vacancies for cyber security positions are there within your Trust, and is their hour capacity affected by a shortage of qualified applicants?

A14 Zero

Q15 Are there mandatory minimum training requirements for those transferred internally to work in cybersecurity within your Trust, and if so, how often is the training updated and revised to reflect the evolving nature of the industry?

A15 There are no minimum training requirements for those transferred internally however each role has a formalised job specification that sets out training requirements.

Q16 How much money is spent by your Trust per year on public relations related to cyber attacks? What percentage of your overall budget does this amount to?

A16 Information not held - We do not have any expenditure on public relations related to cyber attacks.

Q17 Does your Trust have a Chief Information Risk Officer? If so, who do they report to?

A17 Information not held – No such role within the Trust. However, the Trust does have a Senior Information Risk Owner, who reports to the Chief Executive.

Q18 When was the last time your Trust underwent a security audit? At what frequency do these audits occur?

A18 We agree an audit programme with our internal audit provider to cover each financial year and the frequency / schedule will vary from year to year based on the assessment of risk. We are beginning an audit this quarter to comply with our mandatory reporting requirements.

Q19 What is your strategy to ensure security in cloud computing?

A19 We do not have an over-arching strategy re cloud computing security, however we have a process for risk assessment of new, or changes to existing, systems.

Q20 Do you purchase additional / enhanced support from a Supplier for end-of-life software (Operating Systems / Applications)? If so, what are the associated costs per year per Operating System /Application, and the total spend for enhanced support?

A20 Information exempt under Section 31 – law enforcement, specifically section 31 (1) (a) relating to the prevention and detection of crime, as per A3