East London
NHS Foundation Trust

REPORT TO THE TRUST BOARD – PUBLIC
9 MAY 2018

Title	Cyber Security update
Author	Daniel Woodruffe, Chief Information Officer
Accountable Executive Director	Steven Course, Chief Finance Officer

Purpose of the Report:

This report is in response to the requirements laid out by NHS England for Data Security and Protection, and issued to Trusts in April 2018. The paper is an update for the board on the actions regarding Cyber Security the Trust has taken, and plan for addressing future threats. The paper is for information only.

Summary of Key Issues:

Following the well-publicised data security incident (WannaCry) affecting the NHS in May 2017, Trusts have been contacted by NHS England and NHS Digital to provide assurance on the level of Cyber Security in place, and plans to address ongoing threats. Although the Trust was only minimally affected by WannaCry, a significant programme of work has been undertaken to review and upgrade the Trust's Cyber Security infrastructure. This paper highlights for the board the actions taken over the last 12 months, and plans going forward.

Strategic priorities this paper supports (Please check box including brief statement)

Improved patient experience	☒	Service users can be assured of the safe storage of their data
Improved health of the communities we serve	☒	Good Cyber security ensures that the technology that supports service provision is stable and canoperate as intended without interruption from cyber attack
Improved staff experience	☒	Good Cyber security ensures that the technology that supports service provision is stable and canoperate as intended without interruption from cyber attack
Improved value for money	☒	The cost of recovery from cyber attack can be significant, preventative measures represent better vale for money

Committees/Meetings where this item has been considered:

Date	Committee/Meeting
	This paper has not been considered in any other groups

Implications:

Equality Analysis	This document has been assessed for equality impact on the protected groups, as set out in the Equality Act 2010. It is considered there are no direct impact on any of the protected groups.

Risk and Assurance	This paper provides assurance to the board that the cyber security risks faced by the Trust are understood and actions being put in place to address risks identified. This is a rapidly evolving area of risk, and therefore requires an ongoing programme of work to address new issues as they arise.
Service User/Carer/Staff	Cyber security has the potential to affect all staff and service users in the Trust. A major Cyber Security incident (e.g. WannaCry) can have a major adverse impact on staff, patients and reputation of the Trust.
Financial	The Trust has invested a significant sum in addressing cyber security over the past 12 months, and will continue to invest over the 2018/19 financial year. This funding is provided from the IT revenue budgets, through bids to the Trust's capital programme, and (in 17/18) through the award of funding from NHS England.
Quality	N/A

1.0 Background / Introduction

1.1 Cyber Security has long been an issue that IT departments in Trusts have been responsible for, and have been audited on, but has been an area of particular focus following the WannaCry cyber-attack in May 2017, and subsequent disruption to the provision of care in many areas across the country.

1.2 ELFT suffered only a very minor infection of the WannaCry virus – five PCs from an estate of over 5000. These PCs were quarantined and cleaned quickly to prevent spread and infection in other areas.

1.3 Although the direct impact on ELFT was relatively minor, the wider impact of the attack on the NHS led to disruption to care locally in East London (Bart's Health was particularly badly affected). ELFT was also impacted through preventative measures taken by the IT team to avoid infection from other Trusts (disconnection from the internet, shutting down items of critical infrastructure for approx. 24hrs).

1.4 Following the events surrounding WannaCry, both NHS Digital and NHS England have been in regular contact with Trusts to gain assurance on measures to address cyber security risks. This has been helpful in assisting us to audit our infrastructure, provide early warnings of cyber security issues, and to help with funding identified weaknesses in our infrastructure.

1.5 Recently the Trust has been asked to respond to a set of 10 Data Security and Protection Requirements – this paper addresses for the Board the 10 items raised.

2.0 Report Content

2.1 The 10 items set out in the Data Security and Protection requirements issued by NHS England, are set out below, along with the actions ELFT has taken or is planning to take to address the issues raised:

- **Senior Level Responsibility** – A senior executive must be responsible for cyber security. ELFT has appointed Steven Course (CFO and Deputy CEO) as SIRO, and lead for Cyber Security

- **Completing the Information Governance Toolkit** – The Trust has an Information Governance team, managed through the Assurance function, who submit the toolkit annually

- **Prepare for the introduction of the General Data Protection Regulation (GDPR) in May 2018** – The Trust's Head of Information Governance has led preparations for implementation of GDPR

- **Training** – The Trust includes Information Governance training as part of its IG toolkit submission and this is refreshed with all staff annually

- **Acting on CareCERT advisories** – The Trust is registered to receive CareCERT security alerts from NHS Digital, and has a process in place to action the alerts in the required timescale. High severity alerts are acted on within 48hrs, and evidence supplied to NHS England as required. Daniel Woodruffe (Chief Information Officer) is the named lead for the Trust for the CareCERT process and is registered with NHS Digital accordingly.

- **Continuity planning** – The Trust has Business Continuity plans arranged for all teams, and this includes provision for loss of IT services, whether through technical fault or cyber security event. The business continuity process is overseen by the Trust's assurance function.

- **Reporting incidents** – data security incidents are reported by Trust staff via Datix. The Trust CIO reports any significant incidents to CareCERT in line with the agreed guidelines.

- **Unsupported systems** – The IT infrastructure has been audited, and unsupported systems identified. Work is currently underway to upgrade or replace these systems.

- **On-site assessments** – an on-site assessment of data and cyber security has been completed by NHS England's appointed experts (March 2018), and an action plan is currently being worked through (managed by the CIO) to address issues raised. A review of the actions taken is scheduled with NHS England in May 2018.

- **Checking supplier certification** – all IT procurement is managed with procurement colleagues via relevant NHS frameworks where appropriate. Appropriate certification is a requirement of suppliers on these frameworks.

2.2 In support of the 10 requirements outlined above the Trust has undertaken the following Cyber Security actions since the WannaCry incident:

- Registering as a CareCERT early adopter and working with NHS Digital to obtain an audit and early support for cyber security prevention;

- Registering for the Enterprise Threat Detection service – this allows Microsoft and NHS Digital to view all endpoints on the Trust network and identify early any security threats. Issues are therefore rapidly identified and notified to the IT team for remediation;

- Deploying a cloud-based security service, with specific focus on WannaCry type ransomware. External third-party experts therefore manage and maintain our security infrastructure (anti-virus, internet security) and ensure the Trust is up to date on all security provision;

- Securing funding from NHS England to replace old network infrastructure, identified via audit as being out of date and unsupported. This is helping to address one of the major issues identified with out of date equipment.

3.0 Recommendations

3.1 It is recommended the Trust continue to maintain a focus on, and investment in Cyber Security. The IT team will continue to liaise with NHS Digital to audit ELFT's infrastructure and deploy best practice.

3.2 A lead for Cyber Security has recently been identified in the IT team, and has been trained accordingly via a programme funded by NHS Digital. This lead is responsible for carrying out the actions identified in security audits, dealing with CareCERT notifications, and maintaining best practice across the Trust regarding Cyber Security. Regular (weekly) updates are provided to the CIO on activity taken to address identified issues.

3.3 The SIRO will continue to be informed of any significant issues identified regarding Cyber Security

4.0 Action being requested

4.1 The Board is asked to **NOTE** the report for information.