Agenda Item 19d

The Queen Elizabeth Hospital King's Lynn
NHS Foundation Trust

REPORT TO THE BOARD OF DIRECTORS (IN PUBLIC)

RESPONSIBLE DIRECTOR:	REPORT FOR:		IMPACT ON BUSINESS:		
Patrick Johnson, Chief Transformation Officer	Decision		High	Med	Low
	Discussion	✓	✓		
	Information	✓			
LEAD MANAGER:	**REPORT TYPE:**		**BAF REFERENCES & RAG:**		
Mike West, Head of ICT	Strategic				
	Operational	✓			
	Governance		**RELATED WORK: (PREVIOUS PAPERS TO COMMITTEE)**		
PEER ASSIST:	**PEER REVIEW:**				
CQC Domain: (safe, caring, effective, responsive, well-led)					

Meeting Date: 27th November 2018

Report Title: Cyber Security Update

PURPOSE:

To update the Committee on the Trust's current position in relation to cyber security

SUMMARY:

Dionach, on behalf of NHS Digital, carried out a re-assessment of the Trust's current arrangements for tackling cyber security at the end of August 2018. The re-assessment concentrated on areas previously assessed, but with emphasis on Management of Firewalls, Identity & Access Control and Technical vulnerability Review. As expected and previously communicated to Board this identified there were still outstanding actions from their previous assessment in March 2018. Any new actions and risks identified were added to the ICT department's overarching Cyber Action Plan.

The current action plan lists the following outstanding issues which have been identified as critical in the reports and requiring the Trust's timely attention:-

- Inconsistent and Inappropriate Access Control
- Files Contain Credentials in Clear Text
- Weak Domain User Passwords
- Old and Unsupported Versions of Client Software

The ICT Department have agreed a high-level remediation plan for all the Critical and High vulnerabilities with NHS Digital. The department's aim is to complete all of the vulnerabilities and recommendations identified during the NHS Digital technical assessments and recent audits, including low and medium risk items in order to attain NHS Digital's required Cyber Essentials Plus accreditation by June 2021, although this will be extremely challenging if current technical vacancies within the ICT department cannot be addressed.

In addition to the technical assessment and resulting activities, a number of other cyber-related activities have taken place since the last Board report. Namely;

- Phishing Exercise
- Cyber-related Incident Table-top Exercise
- Attendance at Microsoft Advanced Threat Protection (ATP) Event
- Registering of all QEH Windows 10 devices and some Windows 7 devices on ATP website.
- Firewall review and update for best practices
- Audit of the processes for managing IT-related Risk

Progress since last Board update

On behalf of NHS Digital, Dionach revisited the Trust in late August to review the Trust's progress against the action plan from their earlier technical assessment in March 2018. The earlier assessment reviewed existing documentation and technical controls, resulting in recommendations to improve these in accordance with NHS Digital and industry best practices.

In addition to the review of their previous findings, Dionach also concentrated on other key areas;

- Management of Firewalls
- Identity and Access Management (DIAM Review Management)
- Technical Vulnerability Review
- Firewall Rules Management

This identified a number of new actions, and as expected, and communicated in the previous Board paper on cyber security, they also identified that a number of risks from their previous assessment still required action. The findings of the re-assessment were incorporated into the Trust's overall cyber action plan which identifies the following prioritised tasks.

	Priority					Total
	Critical	High	Medium	Low	None	
Number completed	3	8	1	0	0	12
Number outstanding	4	25	31	4	25	89
Total number identified	7	33	32	4	25	101

As can be seen from the above, the ICT Department continues to work on all of the vulnerabilities and recommendations identified during the NHS Digital technical assessments and recent audits, including low and medium risk items, and continue to act on their comprehensive and detailed cyber action plan which includes vulnerabilities at all levels of risk, other recommendations, plus any

incomplete actions from previous cyber reviews and audits.

The 4 remaining critical risks are as follows;

Risk	Description	Target date
Inconsistent and Inappropriate Access Control	Inspection of a number of network shares on the target systems revealed that access control is not applied consistently, and in some cases, access to sensitive data such as patient details or backups could be obtained by a low privileged user.	31/03/19
Files Contain Credentials in Clear Text	A review of the file shares available revealed several files which contained credentials, and other potentially sensitive system information such as connection strings, in clear text.	31/05/19
Weak Domain User Passwords	While many domain accounts were seen to have strong passwords which complied with the current password policy, around 10% (647 out of 6,253 active user accounts) were identified as having very weak passwords.	31/03/19
Old and Unsupported Versions of Client Software	The sample desktops and laptops were found to be running old versions of client software. The following examples were identified as being old versions of client software; 7zip·, Adobe Flask Player, Adobe Reader, Google Chrome, Intel Management Engine, Java	31/03/19

A full version of the complete cyber action plan is attached below;

ICT Cyber Action Plan

Whilst steady progress with the plan continues to be made, the Board needs to be aware ICT are struggling to address the sheer volume of work required in a timely manner, and will be challenged to meet the target for gaining Cyber Essentials Plus accreditation by June 2021, due to the Trust's difficulties with resourcing and recruitment of ICT technicians. The previously approved appointment of a B6 cyber technician has failed to identify a suitable candidate and is about to be re-advertised for the third time. This lack of dedicated cyber resource plus a further 2 senior technician vacancies within the ICT team means it is exceptionally difficult to deliver the department's BAU, capital and cyber agenda, even with the current addition of 2 costly agency technicians.

Discussions are ongoing with partner organisations across the Norfolk & Waveney STP about the possibility of shared cyber resource, although it should be noted that the other NHS organisations in the STP also struggle to recruit and retain IT staff.

NHS organisations have recently been offered further funded support, sponsored by NHS Digital, to equip them to build Cyber resilience and capability across Trusts. This will be in the form of direct on-site support to organisations needing to address critical Cyber security issues to deliver patient and Trust outcomes, whilst continuing to optimise information flows. ICT are currently in discussion with NHS Digital about participating as a pilot in this initiative.

In addition to the ongoing work on the items identified in the cyber action plan, there have also been a number of other key cyber-related activities over the past few months.

Phishing Exercise - July 2018

At the request of the Trust, an external organisation undertook two phishing exercises targeting general and IT staff respectively, to assess levels of awareness and susceptibility. Phishing emails were distributed to Trust staff as follows:

Staff Group	Email Content	Emails Sent
General Staff	Fake ESR notifications.	1499 emails on 3/07/18.
IT Staff	Free technical IT courses.	13 emails on 20/07/18.

It was noted that initial attempts to send large quantities of phishing emails to Trust staff were detected and prevented by Trust IT security solutions. The Trust subsequently changed the configuration of its security controls to enable the phishing emails to be delivered to staff thereby enabling assessment of staff awareness levels.

The exercise identified that the Trust performed better than the 3rd party's phishing system 12-month benchmark, however there is a need for continued improvement and vigilance from both IT and general staff as:

• 8.3% and 14.14% (of IT and general staff respectively) clicked on the link sent to them

• 3.5% of general staff attempted to login via a fake NHS web page.

A report on the findings from the exercise is attached below.

Adobe Acrobat Document

Cyber-related Table Top Exercise - 4th October

At the request of the Trust, an external organisation undertook an appropriate table-top cyber security incident simulation, to assess the Trusts preparedness to deal with such an incident, with the goal to minimise the impact upon service users and the Trust.

Approximately 30 staff from both clinical and operational teams attended the session.

Attendance at Microsoft ATP Event - 8th November

QEH ICT have registered with NHS Digital to provide Microsoft Windows 10 operating system licences, including Advanced Threat Protection (ATP), as this was offered free of charge to local NHS organisations who agree to implement ATP. ATP gives local organisations better cyber security protection in their own right and, as it is connected to the NHS Digital Data Security Centre, it improves cyber security protection across the NHS as a whole.

ICT staff attended a masterclass workshop in London to ensure they get the most from the Trust's allocation of approximately 1700 Windows 10/ATP licenses.

To date over 300 of the estates 1800 devices have been registered and are being protected by ATP. ICT plan to have all devices covered by the end of December 2019. All new devices are automatically registered.

Audit of the processes for managing IT-related Risk – 12-16th November

An internal audit assignment has been carried out by RSM to provide assurance on how the Trust manages the cyber-related risk(s), as there is concern that IT and Cyber risks are not receiving a high enough profile within the Trust and are not considered at relevant decision-making forums.

The Draft report of the findings will be available on 30th November with the final report available on 28th December.

Regular Cyber-related KPI report

ICT have produced a draft report outlining a number of key cyber-related KPI's. This is a requirement for Cyber Essentials accreditation, the new NHS Data Security & Protection Toolkit and at the request of the Trust's Audit committee. The first draft is attached as an appendix to this report. ICT would welcome feedback on the items covered and will amend future reports to accommodate any required changes. It is the intention to produce the reports on a monthly basis, so in future it will identify monthly progress in both tabular and graphical form.

RISK ASSESSMENT (CROSS-REFERENCE WITH RISK REGISTER WHERE APPROPRIATE):

Strategic / External	Operational/ Organisational	Financial	Clinical	Legal/ Regulatory	Reputational / Patient Experience
	√				

RECOMMENDATION/S:

Receive and note the above activities and status on cyber security

Appendix

MONTHLY CYBER PERFORMANCE INDICATORS – OCTOBER 2018

QEH – IT Estate

Desktop PC	1739
Laptop	210
Physical Server	16
Virtual Server	156

QEH Cyber Action Plan

Action/Risk Priority	Open Last Month	Completed this Month	Currently Open
Critical	7	3	4
High	33	8	25
Medium	32	1	31
Low	4	0	4

NHS Digital CareCERT Weekly Updates

CareCERT Type	Alerts Issued	Alerts N/A	Action Required	In Progress	Alerts Completed
Weekly Bulletins	9	0	9	4	5
Threat Notifications	2	0	0	0	2
Special Advisories	0	0	0	0	0

Antivirus

Devices Managed	2162
Devices Up-to-Date	1800
Devices Not Up-to-Date (differ from policy, Out of date or other errors)	362

Obsolete Operating Systems

Desktop/Laptops with Windows XP	13
Servers with Windows Server 2003	16

Trust Laptop Encryption

Laptops with encryption	210
Laptops without encryption	0