Agenda Item 18

The Queen Elizabeth Hospital King's Lynn
NHS Foundation Trust

REPORT TO THE BOARD

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:**		
Mariza Wilson, Interim Head of Digital Services	Strategic				
	Operational	✓			
	Governance		**RELATED WORK: (PREVIOUS PAPERS TO COMMITTEE)**		
PEER ASSIST:	**PEER REVIEW:**				
CQC Domain: (safe, caring, effective, responsive, well-led)					

Meeting Date: 29th January 2019

Report Title: Cyber Security Update

PURPOSE:

To update the Board 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, 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.

This report provides an update on the progress being made to deliver the requirements of the Cyber Action plan and highlight the ongoing challenge to the ICT Department in relation to the lack of dedicated cyber resource.

Progress since last Board update

The ICT Department has continued to work on all of the vulnerabilities and recommendations identified during the NHS Digital technical assessments and audits carried out in 2018.

The following table shows the summary of the number of outstanding actions on the cyber action plan. The ICT Department have completed a further 20 tasks since the last Board report in November 18.

		Priority					Total
		Critical	High	Mediuim	Low	None	
		Nov-18	Nov-18	Nov-18	Nov-18	Nov-18	
Cumulative Actions Completed	Nov-18	3	8	1	0	0	12
	Jan-19	3	10	15	4	0	32
Number Actions Outstanding	Nov-18	4	25	31	4	25	89
	Jan-19	4	23	17	0	25	69
Total number identified		7	33	32	4	25	101

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 cyber action plan continues to be made, the Board needs to be aware ICT are struggling to address the sheer volume of work required. The department 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 VSP have recently rejected the post to be re-advertised due to the period of elapsed time since the business case was approved in Sept 2017 and a request has been made for this business case to be re-visited.

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.

Data Security and Protection Toolkit

The ICT Department are currently focusing on the submission of the ICT/Cyber-related requirements for the new 2018/19 Data Security & Protection Toolkit required to be completed by 31/3/19. A number of the toolkit requirements overlap with the actions on the Cyber action plan. Due to the extent of works required to evidence the assertions within the Toolkit some will not be fully completed, however the Department will provide an Action plan to demonstrate the work being carried out to achieve these.

MicroSoft Windows 10 Advanced Threat Protection (ATP)

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. 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.

Since November the ICT Department have increased the number of devices with ATP from 300 to 1438 of the estates 1800 devices. ICT plan to have all devices covered by the end of December 2019.

All new devices are automatically registered.

Regular Cyber-related KPI report

The attached report shows 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.

Next Steps

- Continue to progress the delivery of the Trust's Cyber Action Plan – prioritising those tasks/risks deemed as critical or high risk, to ensure achieving Cyber Essentials Plus accreditation by June 2021.
- Identify budgetary costs (Revenue and Capital) and timeline for addressing the Trust's Cyber Action Plan.
- Timely submission of all the ICT/Cyber-related requirements for the new 2018/19 Data Security & Protection Toolkit.
- In addition to recruiting to the vacant Cyber Security Technician role within ICT, continue discussions with STP CIO and partner STP organisations regarding STP-based cyber resources.
- Engage with NHS Digital to explore the potential for the QEH to benefit from the recently announced funded support to build Cyber resilience and capability across Trusts.
- Further develop the monthly Cyber KPI report for Board to include trends, performance and any other new/requested metrics.
- Address any actions arising from the recent (October'18) audit of the processes for managing IT-related risk.

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 – DECEMBER 2018

QEH – IT Estate

Desktop PC	1744
Laptop	212
Physical Server	16
Virtual Server	156

QEH Cyber Action Plan

Action/Risk Priority	Open Last Month	Completed this Month	Currently Open
Critical	2	0	2
High	20	2	18
Medium	18	6	12
Low	4	4	0

NHS Digital CareCERT Weekly Updates

CareCERT Type	Alerts Issued	Alerts N/A	Action Required	In Progress (%)	Alerts Completed (%)
Weekly Bulletins	10	0	10	20%	80%
Threat Notifications	2	0	2	n/a	100%
Special Advisories	0	0	0	n/a	n/a

Antivirus

Devices Managed	2220
Devices Up-to-Date	2102
Devices Not Up-to-Date (differ from policy, Out of date or other errors)	396

Obsolete Operating Systems

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

Laptop Encryption

Laptops with encryption	212
Laptops without encryption	0