Agenda Item No.22

NHS
The Queen Elizabeth Hospital King's Lynn
NHS Foundation Trust

REPORT TO THE BOARD [PUBLIC]

RESPONSIBLE DIRECTOR:	REPORT FOR:		IMPACT ON BUSINESS:		
	Decision		High	Med	Low
Ciara Moore, Chief Transformation Officer	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: 31st August 2018

Report Title: Cyber Security Update

PURPOSE:

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

SUMMARY:

An assessment of the Trust's current arrangements for tackling cyber security was carried out during March 2018 by Dionach, on behalf of NHS Digital. The assessment consisted of 2 parts; a Light NHS IT Health Check Report, and a Cyber Essentials Compliance Report. The overall rating was a **FAIL**. It should be noted that all NHS Trusts failed.

The issues which were identified as critical or high in the reports and requiring our timely attention are as follows;

- Old or unsupported operating systems and software i.e. XP, Windows server2003 - CRITICAL
- The PAS transmits patient information in clear text - HIGH
- Services on N3 and PAS have higher risk ports exposed unnecessarily - HIGH
- Management and use of network file shares - CRITICAL
- Examples of weak Passwords - CRITICAL
- Management and issue of privileged accounts - HIGH
- Insufficient patch management - CRITICAL
- Disk encryption - HIGH

The Digital Services Department have agreed a high level remediation plan for all the Critical and High vulnerabilities with Dionach. Following completion of the agreed actions, Dionach will return to site to carry out a re-evaluation of the Trust's cyber preparedness. This is planned for the 28th and 29th of August 2018.

Progress to date

The Digital Services Department have reviewed all of the vulnerabilities and recommendations in their 2 reports, including low and medium risk items, and have produced a comprehensive and detailed action plan to include vulnerabilities at all levels of risk, other recommendations, plus any incomplete actions from previous cyber reviews and audits. Digital Services leads update progress on delivery on a weekly basis with the Chief Transformation Officer and regular updates of the plan are passed to Dionach at least monthly.

While good progress has been made the Board needs to be aware we do not expect to achieve a pass in all areas following re-inspection in August 2018 due to the Trusts resourcing and recruitment of cyber technicians. We will continue to engage external support in the interim, to ensure we manage the Trusts cyber security.

We have a planned cyber-attack table top exercise planned for 22nd August 2018 to test our systems processes and business continuity plans. In addition to this we have planned cyber awareness exercises and tests for the Trust over the coming months.

NHS Digital

The Trust has been successful in securing places on 4/4 NHS Digital pilots for cyber security which will ensure we build a strong cyber secure team, policies, procedures and cyber aware Trust going forward. We are the first in the country to start 2/4 pilots. NHS Digital made a further request that our Trust participate in further trials however at this time due to resourcing we have had to decline. We will however drive the pilots below to achieve exemplar status in these fields for the Trust and with NHS Digital.

Pilot 1: Board Awareness

Our Board attended and indeed are the first board to have access to become GCHQ certified. Board members are to complete on line training to achieve this certificate. This session was delivered on the 15th June 2018.

Pilot 2: Technology and Policy Review

The scope of this pilot intervention is to provide support to review the existing documentation and technical controls resulting in recommendations to improve these in accordance with NHS Digital and industry best practices. The technical controls covered by the review will include the use of patch management systems and the application of any compensative controls. We submitted all relevant documents for review on 17th July 2018.

Pilot 3 National Cyber Security Centre [NCSC] Services

This pilot will provide us with guidance and support on how best to utilise the UK public sector DNS service provided by NCSC. The Webcheck service can be used to look at the organisations URLs and check the domain, certification status, headers and ports before producing an automated report. We are registered for this with a planned assessment in August 2018.

Pilot 4 Central Risk Framework Pilot 4

This pilot has provided us with support to help embed NHS centrally defined risk rating process to prioritise the remediation of discovered vulnerabilities. A consistent risk rating approach will ensure a consistent approach is taken to prioritising and focusing efforts on critical remediation activity. This was completed 4th July 2018.

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 1 – ICT response to questions from Non-Executive Director

(i) the last time our cybersecurity defence systems had a full testing (including penetration) – In March 2018 a "Cyber essentials Compliance Report" and "Light NHS IT Health Check Report" were carried out by Dionach on behalf of NHS Digital. This also tested the external website. The Trust was issued with a "FAIL". ICT are now working through the resulting and agreed action plan.

(ii) how up to date our software patches are – ICT receive regular weekly cyber bulletins from NHS Digital's CareCERT team. This identifies the latest vendor patches and rates them in terms of importance or threat to organisations. These are logged by ICT and assessed for risk, appropriateness, etc. Due to staffing shortages within ICT resources are only available to deal with "critical" patches in a timely manner. Some threats cannot be dealt with until maintenance downtimes. In some cases patches cannot be applied as they are not compatible with 3rd party suppliers' applications.

(iii) what emergency arrangements are in place to ensure patient flow and safety are adequately maintained if all computer systems go down – All departments should have business continuity plans to cater for the loss of Trust IT systems. These are monitored by the Trust's Emergency Planning Manager, Dave Coe. ICT confirm such documents exist for the Trust's key IT systems as part of checks for the IG Toolkit. ICT also have their own BCP to deal with losing IT systems and failures. This is also reviewed at least every year as part of our IGTK submission. The Trust should consider routinely testing these BCP's.

(iv) what arrangements do we have (a) to keep a record of any WiFi enabled bits of equipment (e.g. medical, fridges, vending machines etc...) and (b) ensure we have adequate means of protecting our network(s) in the event of use being made of such devices to gain unauthorised access to them. – ICT do not keep records of all equipment in the Trust which have the capability for communicating via WiFi. Any such devices which wish to connect via the Trust's business network will need to get approval via the relevant ICT policy/process. This process will ensure the device and its usage will not compromise the Trust's network and systems and until such time as approval is given, access to WiFi is not possible. There are no controls to prevent such equipment being connected to the Trust's "Guest WiFi".

Vulnerability Details	Existing Circumstances (technical and organisational background)	Risk	Target Date	Progress Comments (with progress dates)
Old or Unsupported Operating Systems and Software on N3 Network	Some software, such as old operating systems, cannot be updated due to important medical applications. For these systems. operating system patches specially available to the NHS are in user.	Critical	31/06/2018	• Identify systems involved • Create plan for their removal • Where removal is not possible then isolate from other systems wherever possible • Ensure future purchases and contracts include upgrade path, secure software version support, etc
PAS Clear Text Patient Data	The client was surprised and very concerned that PAS network traffic is transmitted in plaintext and thinks that PAS network traffic should be encrypted. Will raise the issue with DXC, though unlikely to be fixed.	High	31/05/2018	• Contact DXC to determine if there is a possible config change or software update • If this not possible then carry out risk assessment to assess risk to Trust • If risk is to high, plan to move to a secure system
Services on N3 and PAS with higher risk ports exposed unnecessarily	The client indicated that many systems require externally available ports to link to other systems. Additionally, it is difficult to communicate with third-party providers to ensure that the systems receive regular patches or push for additional protections such as whitelisting.	High	31/07/2018	• Review all services exposed on N3 and PAS to determine if required and if so at what risk • Where required these systems should be regularly patched and allow only trusted IP's to access them • Where managed by a 3rd party assess their plan for patching and protecting the systems • For every exposed service there should be an owner and justification for doing so
Network shares accessible to low privileged users (passwords in clear text, sensitive patient data, backups, logs, world writable shares, etc.)	The client indicated that while some network shares are reviewed regularly, many are managed entirely by individual departments and may not receive regular security reviews. Additionally, time and resources are very limited, making regular reviews of network shares challenging. The client believes that, in general, clinical data should not be on network shares and that ICT Department has been arguing for greater security restrictions.	Critical	31/07/2018	• Review applied permissions of all network shares • Check data stored in shares and where PID is identified ensure appropriate access control is applied • Create formal procedures for regular reviewing of shares
Weak passwords (Domain Users and SQL Databases)	The client indicated that while a password policy does exist, many weak passwords appear to be 1st-use passwords that must be changed on first login. Therefore, the users to whom these passwords belong have never logged in. Under current policy, all accounts that have not been used in 2 years are reviewed and deleted, meaning these accounts are likely under 2 years old.	Critical	31/07/2018	• Carry out review of all relevant user accounts and related passwords• Create and implement procedures to carry out reviews on a regular basis• Consider setting stronger default and one-time use passwords (use passphrases instead of weak one-time passwords)• Consider requiring fewer password changes and instead require stronger longer passwords

Accounts with unnecessary privileges (Domain Admins, Local Admins, Enterprise Admins)	The client has previously raised concern about overly privileged accounts, particularly service accounts. While IT staff need admin accounts and KLW accounts should not have internet access, many service accounts may not need administrator rights.	High	31/06/2018	• Set a policy for admin accounts to used for “admin” only and where possible grant access to the least privileges • Regularly review the creation and use of admin accounts
Insufficient Separation of Privilege	The client indicated that account privileges are regularly reviewed, but in some cases users use admin accounts for everyday use. These accounts will be reviewed. Additionally, administrative accounts should not have internet access.	High	31/06/2018	• Set a policy for admin accounts to used for “admin” only and where possible grant access to the least privileges • Regularly review the creation and use of admin accounts
Insufficient Central Patch Management	The client indicated that only Microsoft updates, not third-party application updates, are centrally managed. While not all systems are on WSUS, some systems are not on WSUS purposefully so they are not updated mistakenly. Other systems are not on WSUS because the WSUS system is still in progress and resources are limited.	High	31/06/2018	• Configure WSUS system to ensure that all active hosts are covered with central patching, and regular audit their coverage • Consider removing 3rd party software which is not required to reduce window of attacks • Create procedures to use automated scanning tools to check correct installation of updates
Missing Microsoft critical security updates, including MS17-010 (WannaCry patch) on desktops and laptops	The client indicated that Microsoft updates are currently centrally managed by WSUS. However, the laptops provided to Dionach were not patched along with other computers on the network, as they have been unused for some time and the WSUS system is still in progress. Additionally, some critical system cannot receive updates.	Critical	31/06/2018	• Configure WSUS system to ensure that all active hosts are covered with central patching, and regular audit their coverage • Consider removing 3rd party software which is not required to reduce window of attacks • Create procedures to use automated scanning tools to check correct installation of updates
Missing Non-Microsoft critical security updates on desktops and laptops: Java, Adobe Products, Intel Management Engine, 7zip, etc.	The client indicated that third-party application updates are not centrally managed due to the lack of resources.Additionally, the latest version of Java is not officially supported by many NHS applications.	Critical	31/06/2018	• Configure WSUS system to ensure that all active hosts are covered with central patching, and regular audit their coverage• Consider removing 3rd party software which is not required to reduce window of attacks• Create procedures to use automated scanning tools to check correct installation of updates
Workstations Not Protected by Disk Encryption	The client indicated that desktops are not normally encrypted while laptops are generally encrypted, the laptops provided to Dionach were not encrypted at the time of testing because they were test laptops used only in ICT.	High	31/05/2018	• Ensure all laptops are encrypted • Confirm if NHSD policy is for all devices to be encrypted and if so encrypt all Trust desktops