Healthier Communities, Outstanding Care

NHS Sherwood Forest Hospitals NHS Foundation Trust

Board of Directors - Cover Sheet

All reports MUST have a cover sheet

Subject:	Cyber Security & COVID-19	**Date:** 30/04/20	
Prepared By:	Deborah Poznanski – Head of Governance & Assurance		
Approved By:	Jaki Taylor – Director of NHIS		
Presented By:	Jaki Taylor – Director of NHIS		
Purpose			
To provide information to the Board of Directors.		**Approval**	
		Assurance	
		Update	X
		Consider	

Strategic Objectives				
To provide outstanding care	**To promote and support health and wellbeing**	**To maximise the potential of our workforce**	**To continuously learn and improve**	**To achieve better value**
X		**X**		**X**

Overall Level of Assurance				
	Significant	**Sufficient**	**Limited**	**None**
	X			

Risks/Issues	
Financial	Should there be a cyberattack and the Trust found not to have the correct controls in place the Fines can be up to £19m
Patient Impact	Without appropriate Cyber Security (software, hardware and controls) in place the risk of patient harm is significant as it will almost certainly render computer systems and services used by the Trust unavailable and therefore patient records and results may not be available or may be compromised.
Staff Impact	Without appropriate Cyber Security (software, hardware and controls) in place the risk of patient harm is significant as it will almost certainly render computer systems and services used by the Trust unavailable and therefore patient records and results may not be available or may be compromised.
Services	Without appropriate Cyber Security (software, hardware and controls) in place the risk of patient harm is significant as it will almost certainly render computer systems and services used by the Trust unavailable and therefore patient records and results may not be available or may be compromised.
Reputational	Without appropriate Cyber Security (software, hardware and controls) in place the risk of patient harm is significant as it will almost certainly render computer systems and services used by the Trust unavailable and therefore patient records and results may not be available or may be compromised.

Committees/groups where this item has been presented before

N/A

Executive Summary

The National Cyber Security Centre (NCSC) has assessed that COVID19 presents an increased risk of a cyber-attack to healthcare services. The UK health sector is **highly likely** now considered a high value target by a range of malicious cyber actors. Ransomware is a particular concern right now; it has been used already during COVID-19 against healthcare in other countries and the criticality of the NHS right now makes it an attractive target to cyber criminals. Any type of cyber campaign could have a devastating impact on the NHS right now and therefore it is imperative that cyber security is strengthened across the entire NHS.

Nigel Sturrock, the NHS England and NHS Improvement Medical Director and Chief Clinical Information Officer has written on the 16th April to all NHS organisations to advise them of a number of steps that health organisations need to be taking to ensure good cyber security hygiene and also to inform them of various NCSC and NHS Digital initiatives that are available to support organisations.

The letter also outlines 5 key questions leaders might want to ask their organisations and provides the Nottinghamshire Health Informatics Service (NHIS) response to the recommendations and initiatives noted in the letter.

Background

Cyber Security and COVID-19

Trust response to 5 Key Questions

1. **Does our organisation have adequate backups in place, especially for our critical systems to enable us to restore data quickly if we are hit by Ransomware? Are backups stored correctly and regularly updated.**

   Daily back up checks on operational logs are undertaken on all systems and failures identified and resolved. A procedure is in place to retain and swap backup tapes and verifying that backup jobs have run. As part of NHIS ISO 27001:2017 certification the back-up process is assessed and audited annually, and the last audit was compliant as of December 2019. Resiliency exists across the network with backup being replicated and held separately to the data centre.

   Currently the backup infrastructure is located within Kings Mill's two data centres and a third Network Hub room. The roadmap is due to setup the VxRail datacentre environment at an offsite location and once in place we will seek to replicate backup sets offsite. This will provide enhanced DR functionality for critical services by replicating their virtual servers in their entirety.

2. **Is our organisation up to date applying critical security patches?**

   NHIS implements patch management according to best practice to ensure that security updates are applied in a timely manner to maintain the security of the network. Application of the patches is validated and verified using network scanning tools and Hygiene Reports produced monthly to illustrate patching levels and compliance across all devices and servers.

   Intermittent checks are undertaken to ensure that the patches continue to be applied and are functioning correctly.

   The Hygiene Reports are provided to the Cyber Security Assurance Programme Board members and any exceptions are identified and compliance monitored. The Hygiene Reports now include Medirest server patching stats.

   For the end of March 2020, server patching has increased by 1.54% and desktop patching is down by 1.48%. NHIS is seeing a larger amount of device inactivity due to disruption in customer COVID-19 response and as such a higher number of devices are not active and able to take security updates. Once the device is attached to the network, the patch will be applied and the NHIS scanning systems will monitor uptake.

Currently the Cyber team are dealing with an increase of approximately 7 alerts per day within Sophos Central, which need investigation and remediation (this is across the whole NHIS estate).

See Appendix 1

These incidents can vary from malware within webpages categorised as Low Threat Severity to Malware on devices, usually categorised as High to Medium Threat Severity. Recently and additional security layer was activated with Machine Learning being activated and this is now detecting Potentially Unwanted Applications (PUA). All PUA has to be confirmed to be deleted or whitelisted to allow the application to run.

All threats have been resolved either by an automated process or where required by a manual process involving locating and remediation of individual devices. Any users involved in an incident that requires manual intervention are being notified after the eradication of the threat. The Cyber Security team are constantly monitoring any evolving threats and undertaking the necessary remediation. Anti-malware on the firewalls is UpToDate and on access scanning is in place. The organisation also responds to the NHS Digital security alerts and remediates where necessary.

3. **Does our organisation operate any unsupported operating systems without other mitigations in place to protect them? If we have windows 7, have we activated extended support on all devices?**

There are some unsupported operating systems across the estate. There are 9 XP devices at SFHT, and all have projects in place to either decommission or replace and risk assessments are in place.

There is also a plan in place to implement micro-segmentation which segments unsupported operating systems away from other systems. There are some Windows 7 devices in the organisation, extended support has been activated for all of these machines and the devices receive the appropriate security patches.

NHS Digital has now extended the timeline for Windows 10 implementation until the end of June 2020 due to the operational impact of COVID-19. Excellent progress was made until resources were diverted onto building laptops. Only 664 devices (5.45%) across the full NHIS estate now need to be upgraded.

Windows 10 will remain on hold until the COVID situation passes. Some Windows 7 devices are being used for remote working but given the current situation it's appropriate to continue with remote working and the devices continue to receive security updates. An assessment is being conducted to see if PC's can be built remotely, swapped out at site and then any remedial work conducted remotely without introducing too much risk to staff.

4. **Has our organisation rolled out Advanced Threat Protection (ATP) as far as possible across the estate to take advantage of the additional protection it brings?**

ATP is rolled out to 97% of the estate, as we are building more Win 10 devices and they are in stock awaiting them to be onboarded.
Out of the remaining 292 desktops: 107 are Windows 10 that will onboard as soon as online and in reach of ATP. 142 x Windows 7; and 34 x Windows 8.1 devices will be decommissioned and replaced with Windows 10 devices over time. Windows XP legacy devices are not ATP compatible,

but still receive the necessary updates.

5. **Could we onboard quickly to NHS Secure Boundary? Weekly webinars available and access to funding to address infrastructure barriers.**

   NHS Secure Boundary could be onboarded quickly. An investigation is currently underway to establish the benefits that NHS Secure Boundary will provide as the features provided are already available with existing products in use, and also to establish how it would operate with existing products.

   NHIS were implementing firewalls at GP (and Community sites), planned for August 2020. This is being brought forward due to the increased cyber risk due to COVID-19.

Further Cyber Security Activities

The partner-wide Cyber Security Strategy has been delivered through the Cyber Security Assurance Programme and an approach being considered across the Local Health and Care Record (LHCR) to ensure that the progress made through the programme is sustained. An updated cyber security approach is being developed in line with the Integrated Care Partnership (ICP) data, analytics, Information and Technology Strategy. The current strategy has delivered a number of initiatives in line with national cyber security recommendations including:

- Web-filtering across partner organisations following a partner-wide policy application of best practice
- Removable media programme which prevents unencrypted devices from attaching to the network where a security risk is identified
- NHIS specialist Cyber Security team providing monthly hygiene reports showing patching and vulnerability status across the estate
- User awareness campaigns; best practice guidance and regular Cyber Newsletters
- Next generation firewalls in place across the local network – with additional firewalls being implemented to enable segmentation of the network.
- IT Health Dashboard monitoring to scan the network and identify devices requiring security updates and patches
- Delivery of the latest operating system for computers and identification and risk assessment of devices out of support, identifying Information Asset Owners of each.

Conclusion

The NHS has undertaken a major cyber security programme over the last two years, both nationally and locally. Every month over 21 million incidents of malicious activity on the national network are stopped, and more than half a billion emails every three months.

NHIS continues to follow our usual protocols and closely monitoring the situation with respect to the security of the network and infrastructure.

NCSC issued an advisory on 9th April outlining COVID-19 misuse. Although there has been an increase in the number of phishing e-mails received and the number of links that users have clicked on the products and services that are in use have managed to successfully capture any malicious software to minimise the impact.

A number of technology solutions are being implemented across the trust as a result of COVID-19 (see Appendix 3). Cyber Security is a key factor in any implementation, and all implementations are assessed and reviewed with security in mind.

This paper will provide the Board with the assurance that the Trust has in place adequate cyber security considerations and a fresh cyber-attack would not result in a catastrophic event across the health economy due to the work undertaken to strengthen the cyber security posture since the ransomware attack in May 2017 and implementation of robust cyber security measures locally.

Appendix 1 – Number of Malware Attacks Graph
Appendix 2 – Cyber and COVID Letter
Appendix 3 – SFH COVID-19 Digital Initiatives

28th April 2020

Recommendation

NOTE the attached paper and receive ASSURANCE of appropriate cyber security arrangements.