Sherwood Forest Hospitals
NHS Foundation Trust

Board of Directors Meeting in Public - Cover Sheet

Subject:	Cyber Security Board Responsibilities	**Date:**	
Prepared By:	Jacqueline Taylor, Director of NHIS		
Approved By:	Peter Wozencroft, Director of Strategic Planning and Commercial Development		
Presented By:	Peter Wozencroft, Director of Strategic Planning and Commercial Development		

Purpose		
The purpose this paper is outline the Board responsibilities with respect to Cyber Security, as outlined in the Lessons Learned review of the WannaCry Ransomware cyber-attack report that was commissioned by NHS England.	**Approval**	
	Assurance	**X**
	Update	
	Consider	

Strategic Objectives				
To provide outstanding care to our patients	**To support each other to do a great job**	**To inspire excellence**	**To get the most from our resources**	**To play a leading role in transforming health and care services**
X	**X**		**X**	**X**

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

Risks/Issues	
Financial	Potential for fines of up to £500k to be imposed by the ICO for breach of the Data Protection Act; aftermath of an information security breach could involve considerable costs in remediation and resources
Patient Impact	Potential for causing distress to individuals if sensitive personal information is not protected; if patient health records aren't available when needed it could delay diagnosis and treatment. Significant disruption could be experienced where network services and clinical systems are not available due to a successful cyber security attack.
Staff Impact	Potential for causing distress to individuals if sensitive personal information is not protected; inefficient management of information can create additional staff workload.
Services	A cyber security incident or records management issue could have a disruptive impact on multiple services.
Reputational	Failure to comply with information governance legislation, regulations and guidance could lead to regulatory action and significant damage to the Trust's reputation.

Committees/groups where this item has been presented before

A summary of the recommendations of the Lessons Learned review of the WannaCry Ransomware cyber-attack has been reviewed by the Cyber Security Assurance Programme Delivery Group and appropriate actions added to the workplan.

The Sherwood Forest Hospitals NHS Foundation Trust Executive Team have NOTED the report

Executive Summary

In May 2017, a global ransomware attack known as WannaCry affected a wide range of countries and sectors. Although WannaCry impacted on the provision of services to patients, the NHS was not a specific target. The NHS responded relatively well to this attack, with no reports of harm to patients or of patient data being compromised. However, there was still an impact upon a number of organisations, where they were not infected by the ransomware, but where systems were taken down as a precaution to prevent the potential spread of an infection.

The incident highlighted a number of areas for improvement both within NHS organisations and also across the system as a whole. NHS England, with the Department of Health and Social Care, produced a lesson learned report, which outlined a number of recommendations that NHS organisations at all levels should undertake[1].

Within those recommendations a number of responsibilities were identified for organisational boards, as well as recommendations for NHS Digital and the NHS Chief Information Officer to strengthen the resilience and accountability across the Health and Social Care system in the event of a further attack or major disruption to services.

This report provides a brief summary of the recommendations that apply to NHS organisational boards only, to raise awareness to the Sherwood Forest Hospitals Board and present current compliance with the recommendations.

[1] NHS England WannaCry Lessons Learned Report

WannaCry Lessons Learned Report Recommendations

The Lessons Learned review of the WannaCry Ransomware cyber-attack clearly identifies the need for senior leadership and board level accountability for cyber security in every health and care organisation. The recommendations below apply to NHS Organisational Boards.

Recommendation 1:

All NHS organisations are to develop local action plans to achieve compliance with the Cyber Essentials Plus standard by June 2021, as recommended by the National Cyber Security Centre (NCSC).
The UK Government has introduced a Cyber Essentials and Cyber Essentials Plus scheme, which is a certification scheme setting a basic level of cyber security. NHIS has already obtained Cyber Essentials certification from September 2016 and renews this annually.

The Cyber Essentials Plus is essentially a penetration test that tests the network infrastructure against a set of pre-defined standards. Nottinghamshire Health Informatics Service (NHIS) is investigating the application of the standard with their security partners, IT Health, and further information and advice on the application of this to the Trust is pending from NHS Digital.

Current Progress	Timescale	Compliance
Further advice required from NHS Digital on the application of this standard across NHS organisations	NHS Digital timescale - June 2021	COMPLIANT
NHIS has obtained Cyber Essentials Plus certification	NHS Digital timescale - March 2020	COMPLIANT

Recommendation 3:

The SIRO on behalf of the board, should be charged with ensuring that the 10 information security standards are followed throughout their organisation.

The NHS Digital Information Governance Toolkit has been replaced by the Data Security and Protection Toolkit and all NHS organisations are expected to submit a compliant response to the standards by March 2019. The new version is based on the 10 Data Security standards as set out in the Caldicott Review of 2016.

There are a number of technical elements that require an assertion or evidence to achieve compliance, which will be provided to the Trust by Nottinghamshire Health Informatics Service (NHIS).

The Information Governance team is managing the response to the Data Security and Protection Toolkit and will submit a baseline performance report to the Information Governance Committee at the end of October 2018.

Current Progress	Timescale	Compliance
The Trust is working towards the completion of the Data Security and Protection Toolkit	March 2019	COMPLIANT

Recommendation 5:
Organisations should ensure every NHS Board has an executive director as data security lead. Cyber security risks should be reviewed regularly by the Board in order to understand the risks posed to the organisation

The Board Executive lead needs assurance from the organisation that key information assets are identified and their vulnerability to attack has been assessed. This would be actioned through mapping of information flows and refresh of the current Trust asset register which will be managed by the Information Governance team as part of compliance with the Data Protection Act 2018 (GDPR) obligations. Information Asset Owners (IAOs) will be supported by the Information Governance team as they roll out refresh of the Information Asset Register and Data Flows as part of the organisations compliance with the Data Security and Protection Toolkit to March 2019.

Nottinghamshire Health Informatics Service (NHIS) has set up a Cyber Security Assurance Programme which reports through the NHIS Partnership Board to each partner organisation. Hygiene reports are presented monthly, which set out the current situation with regard to system security patching and updates and identifies any security risks posed by unsupported software and systems. Within the Trust, the Programme reports to the Information Governance Committee and Shirley Higginbotham is the nominated data security lead who attends the Cyber Security Assurance Programme.

Current Progress	Timescale	Compliance
The Trust is working towards the completion of the Data Security and Protection Toolkit, which includes Information Asset Register review and Data Flow Mapping	March 2019	COMPLIANT

Recommendation 8:
Organisations should ensure that disaster recovery plans include cyber security and that organisations assess the impact of a loss of IT services would have on the healthcare system.

NHS organisations are advised to collaborate with local Warning Advice and Reporting Point (WARP) groups to share trusted up-to-date advice on information security, cyber threats, incidents and solutions. This is being taken forward by the Trust Emergency Planning Lead. All SFH departments / services have business continuity arrangements in place specifically for a loss of IT systems, as recommended in NHS EPRR Guidance (2015). These arrangements are produced to the ISO22301 Business Continuity Standard and are developed following a formal Business Impact Analysis.

NHIS has developed and tested an Incident Response Plan to ensure the network can be segmented where possible should a successful cyber-attack occur, which will significantly minimise the impact and limit the attack spreading to multiple sites - for example the use of firewalls at network boundaries.

NHIS has agreed with partners the operation of an incident management response in order for NHIS to ensure all risks and priorities can be taken into account and are working with the local Emergency Planning Leads to test these plans.

Current Progress	Timescale	Compliance
The Trust has a Business Continuity Plan in place	December 2018	COMPLIANT
NHIS has developed and tested an Incident Response Plan	December 2018	COMPLIANT
The Trust is working with local Emergency Planning leads across the wider health and social care system.	March 2019	COMPLIANT

Recommendation 11:

Health and social care organisations must invest in the appropriate IT infrastructure, tools and resources. Boards should assure themselves that they have sufficient quality and capable IT technical resources to manage and support their local IT infrastructure, systems and services

The Cyber Security Assurance Programme (CSAP) has membership from all NHIS partners and is ensuring the delivery of the NHIS Cyber Security Strategy including actions and lessons learned from the cyber-attack in May 2017. The programme is led by NHIS and provides ongoing assurance to the Information Governance Committee.

External and internal vulnerability testing has taken place (NHIS engaged with the NHS Digital delivery partner – Dionach to do external penetration testing) and NHIS has implemented a remediation plan to address identified gaps in controls.

NHIS is maintaining ISO27001 certification, which demonstrates compliance with a recognised information security accreditation.

The report recommends that pooled resourcing arrangements are formalised and captured in STP or ACS wide continuity plans in relation to system-wide cyber-attacks. This is being considered as part of the Nottinghamshire Digital Collaborative between NHIS, Nottingham University Hospitals and Nottinghamshire Healthcare Trust.

Current Progress	Timescale	Compliance
NHIS is maintaining ISO 27001 Certification	April 2019	COMPLIANT
Annual penetration testing occurs, and remediation plans are in place	April 2019	COMPLIANT
Pooled resourcing arrangements are formalised across the ICS footprint	March 2019	PARTIALLY COMPLIANT

Recommendation 13:

Boards for NHS organisations should undertake annual cyber security awareness training.

This should be in addition to mandatory information governance training and NHS England has suggested suspension of IT access for any executive who fails to complete annual cyber security training

All staff should have a mandated standard level of awareness and training in cyber security, with the WannaCry report also stipulating that Board members should have annual cyber security

awareness training.

NHS Digital has developed a Data Security Awareness e-learning package (level1) which is in widespread use across NHS Organisations. Where organisations are developing their own internal training (either e-learning or face-to-face) then the course content must contain an equivalent cyber security training content. The current SFHT package is offered through the Sherwood e-Academy and is the designated mandatory training package for staff to complete and on induction to the organisation. The content of this package has been aligned to the NHS Digital training package and includes both cyber security equivalent and GDPR content.

The Information Governance team are working with Nottinghamshire Health Informatics Service (NHIS) to review external cyber security training and awareness options to ensure that the content continues to meet best practice and is in line with the National Cyber Security Centre (NCSC) offerings.

NHS England are still working to define the standards and expectations of Boards through the national cyber expert working groups and set the level of training and awareness required.

Current Progress	Timescale	Compliance
Cyber security is included as part of the annual mandatory staff training	March 2019	COMPLIANT
All staff to have the appropriate level of cyber security training relevant to their role (TNA)	March 2019	COMPLIANT
Board members should undertake annual cyber security training	March 2019. NHS Digital have yet to define this standard	PARTIALLY COMPLIANT

References

https://www.nao.org.uk/report/investigation-wannacry-cyber-attack-and-the-nhs/

https://www.gov.uk/government/news/national-data-guardian-2017-report-published

The Board is requested to NOTE the above report