NHS Blood and Transplant

NHSBT BOARD MEETING

March 2017

'Securing Cyber Resilience in Health and Care: A Progress Update'

1. Status – Official

2. Executive Summary

On 1 February 2018 the Department of Health and NHS Digital wrote to NHSBT Board members to update them on progress towards improving cyber resilience in the NHS and Social Care space.

There are two actionable elements within the letter:

1. A request for Boards to familiarise themselves with the 22 recommendations from the review of the 2017 'WannaCry' incident, presented to the NHS England Board on 8th February, and;
2. A list of questions that Boards should ask themselves, in relation to their own organisation's stance towards cyber resilience.

This paper is therefore intended to provide the Board with:

- a breakdown of activities and stances for all *relevant* observations, and
- assurance that the cyber stance at NHSBT is *at least consistent with the minimum requirements outlined in the letter.*

3. Action Requested

The Board is asked to:

- **Review NHSBT's current position in relation to the recommendations in the NHS England Board report**
- **Note that the annual NHS Digital Information Governance Toolkit is being replaced,**
    - **with provisions in this paper likely to be core elements of assurance**
    - **with some elements possibly becoming future statutory obligations**
- **Continue to sponsor, encourage and mature the cyber security Stance within NHSBT, particularly given the extensive ongoing modernisation of the technology estate.**

4. Purpose of the paper

4.1. This paper is to provide assurance to Board of the relevant elements outlined in the letter to Non-Executive Directors from the Department of Health in relation to cyber security and resilience, and the recommendations presented to the NHS England Board in response to the WannaCry incident.

4.2. For completeness, a full analysis of all requirements has been compiled by NHSBT staff, and NHSBT has been found to be aware of all activities in the sector, whether or not NHSBT is directly required to respond.

5. Background

5.1. The NHS Information Governance Toolkit is being replaced from 2019 with a new Cyber Toolkit. This will require NHSBT to implement and be able to evidence the implementation of cyber security standards on a whole range of elements. NHSBT staff are actively engaged with NHS Digital in reviewing these requirements in order to ensure that NHSBT is able to respond positively when the toolkit is launched.

5.2. The implementation of the General Data Protection Regulation and the EU Networks and Information Systems Directive requires NHSBT to implement a set of cyber controls and processes and procedures to underwrite good information security hygiene within the digital estate.

5.3. A series of reviews are underway within the sector which will result in the further requirements in the future.

5.4. The 2017 'WannaCry' incident exposed a number of weaknesses in maturity of approach within NHS Bodies which exposed digital assets to unnecessary risk. These were summarised in the report to NHS England's Board on 8th February 2018, with 22 recommendations for improvement made.

5.5. The letter written to NHSBT non-executive directors updates guidance on a wide range of cyber security elements (including the above) which NHS Bodies should be aware of and factoring in to their own cyber assurance programmes.

6. Proposal

6.1. Appendix A contains the joint letter from Department of Health and Social Care, and NHS Digital and Appendix B identifies how Board members may be satisfied in regards to the questions posed.

6.2. The following notes are a direct response to the applicable findings of the 2017 'WannaCry' cyber security incident report to the NHS England Board.

No.	Recommendations	NHSBT Response
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 NCSC. These plans will be provided to NHS Digital on behalf of the Chief Information Officer for health and social care by 30 June 2018. NHS Digital should produce a framework to support organisations, drawing on security assessments undertaken to-date	NHSBT is aware of the elements of the Cyber Essentials Plus key themes. NHSBT's Security stance at least meets, and often exceeds the requirements. 06/2018 submission will be provided once the new Cyber Toolkit is released by NHS Digital.
2	In the first quarter of 2018/2019 financial year, the CIO for health and social care will convene an expert panel to define and consult on a set of IT infrastructure, application and service management guidelines for organisations hosting clinical systems and patient data.	The outcome of the Expert Panel is awaited.
3	By 31st March 2019, all health and social care organisations that provide NHS care through the NHS Standard Contract must provide NHS Digital on behalf of the CIO for health and social care details of their position against the DSPT. This will help audit compliance against the NDG’s 10 security standards and CQC’s well-led KLOE. Position statements are expected to include an action plan setting out how organisations will address any shortfalls in their compliance and plans for the forthcoming GDPR.	NHSBT does not provide care through the NHS Standard Contract. However, NHSBT does complete the Data Security Protection Toolkit (the replacement for the Information Governance toolkit) and is reviewing the prototype toolkit requirements.
4	Research will be commissioned by the CIO for health and social care to build an evidence base to understand the level of cyber security maturity in social care organisations. This research will be used to identify where additional support to the social care sector can be most effective.	The outcome of the research is awaited.
5	All NHS organisations are to ensure that every board has an executive director as data security lead, cyber security risks are regularly reviewed by the board, appropriate counter-measures are in place to mitigate and response plans are in place to address service restoration in the event of a successful attack. As CCGs are the responsible commissioner for GP IT services for general practice, a board member or equivalent senior manager should fulfil this role for CCGs.	NHSBT meets this requirement. Aaron Powell is the responsible director.
6	Health and social care organisations should ensure that local contracts, processes and controls are in place to manage and monitor third party contracts for local IT systems, and that the provisions for software updates and business continuity are understood. CCGs are responsible for this for GP practices.	NHSBT manages and monitors third party performance. Provisions for software updates and business continuity are well understood and built into comprehensive and matured processes and procedures. Business continuity provisions for third parties are reviewed on a risk-basis to ensure continuity of NHSBT’s services.
7	During the first quarter of the 2018/19 financial year, a working group will be established by NHS Digital on behalf of the Chief Information Officer for health and social care to define standards around the management and patching of	The outcome of the Working Group is awaited, although NHSBT is undertaking robust internal activities to identify and assess gaps.

	diagnostic equipment.	
8	Local organisations' business continuity and disaster recovery plans should include the necessary detail around response to cyber incidents, and must include a clear assessment of the impact of the loss of these services on other parts of the health and social care system. In addition, these plans must identify critical third party services (provided by other health, social care and private sector organisations), setting out the impact of the loss of these services on their operations and necessary business continuity actions required to address the loss of such services. Plans should be regularly tested across local areas both with the NHS and its partners, and reviewed and updated locally with board level oversight.	NHSBT meets this requirement. Business continuity requirements are assessed on a service by services basis, dependent upon their business criticality (which is a formal assessment).
9	It is recommended that NHS Digital appoint a system-wide Chief Information and Security Officer (CISO). In addition, it is recommended that NHS Digital appoints a dedicated Cyber Security Lead working across NHS England, NHS Improvement and other partners such as local government in each of the NHS England regions (North, Midlands and East, London, South East and South West).	This is a recommendation for NHS Digital and NHSBT is aware of appointments being made.
10	We recommend that, where they exist, NHS providers join and collaborate with local Warning Advice and Reporting Point groups to share trusted up-to-date advice on information security, cyber threats, incidents and solutions.	NHSBT receives, processes and shares intelligence with a wide spectrum of organisations. It does not belong to a Warning/Reporting Group, but leverages close relationships with many NHS touchpoints as required.
11	In addition to local boards assuring themselves that they have sufficient quality and capable IT technical resources to manage and support their local IT infrastructure, systems and services, we recommend that pooled resourcing arrangements are formalised and captured in STP or ACS wide continuity plans in relation to system wide cyber-attacks.	NHSBT meets this requirement, and has no Shared Resources.
12	Professional community network models should be encouraged for cyber and information security, working in conjunction with organisations such as NHS Digital, The British Computer Society, Health Education England and the NHS Digital Academy.	NHSBT meets this requirement and NHSBT staff are actively engaged in a range of networks
13	Boards for NHS organisations should undertake annual cyber awareness training and further consideration should be given to the training needs for social care providers arising from recommendation 4. The standards for training will be established nationally in 2018 by the CIO for health and social care. In addition, whilst we do not formally recommend it, all organisations should consider whether access to IT systems and services should be removed from members of staff who have not successfully completed this mandatory training.	The publication of Standards is awaited. NHSBT enjoys active Board-level sponsorship of the cyber-security agenda with high levels of engagement.

14	In addition to mandatory and statutory training, organisations should ensure that their staff receive regular and targeted cyber and information security awareness training appropriate to their job role. This may range from internal phishing attacks to test the awareness of staff to the danger of opening spam email, through to specific training associated with the management of cyber incidents.	NHSBT meets this requirement. Plans are at an advanced stage to introduce simulated phishing and supportive training.
15	It is recommended that NHS Digital proactively publish guidance about the CareCERT service and maintain a clear and consistent view of the technology landscape across local organisations. In the longer term, NHS Digital should have the ability to isolate organisations, parts of the country or particular services in order to contain the spread of a virus during an incident.	This recommendation is directed at NHS Digital. NHSBT will participate as required.
19	It is recommended that an annual national cyber rehearsal is undertaken by the DHSC, NHS England, NHS Improvement and NHS Digital, and that regional and local organisations similarly undertake regular tests of their EPRR in the event of a cyber incident.	NHSBT is compliant with this element. An annual Emergency Response Planning exercise takes place at NHSBT consistent with the requirement outlined and as part of ongoing ISO22301:2013 certification needs.
20	The DHSC, NHS England, NHS Improvement and NHS Digital should develop joint protocols for clear and consistent communications to local organisations to provide updates, advice and guidance incidents and for local reporting. This should include working with local organisations and relevant networks to identify alternative communicate channels in the event of distribution to standard channels.	NHSBT will support this initiative as required. NHSBT has internal processes which work well for the organisation, as part of its own Business Continuity planning.
21	NHS Digital should develop their on-call and major operating guidelines to ensure the right expertise and seniority of decision making is available in the event of another cyber attack. NHS Digital's contact centre also needs to be sufficiently resourced to address information requests during an incident.	NHSBT will watch development of this capability and ensure its own processes and procedures are consistent with any new requirements which may surface. NHSBT already has a 24x7 on-call capability for its own Business Continuity programme, as well as an IT Critical Incident Management rota and Gold Director-On-Call rota. NHSBT is developing a checklist of 'potential actions' to be taken in the event of a cyber incident to assist in decision making.
22	CSUs must be cyber accredited and responsible for coordinating a cyber response across primary care and CCGs. All parts of the country must be covered by a CSU and all GP practices and CCGs must receive IT support from cyber accredited suppliers. NHS Digital should draw up a national response protocol and all approved IT suppliers must comply with it to ensure 24/7 on call care and linkages to CSUs.	Whilst NHSBT is not part of this specific requirement, NHSBT will watch developments in this area and ensure that its' own training and accreditation remains consistent with the overall aims and objectives of this element.

6.3. Recommendations 16 to18 relate to NHS England and NHS Digital's Emergency Preparedness Resilience and Response plan. NHSBT has its own such plans and discussions are underway as to the extent to which cyber resilience should be tested through it.

Author	**Responsible Director**
Barry Richardson	Aaron Powell
Head of Information Security	Chief Digital Officer

02 March 2018

Appendices:

Appendix A: Letter to NHSBT from Department of Health and Social Care, and NHS Digital

Acrobat Document

Appendix B: Responses to formal questions:

No.	Key Area	NHSBT Response
1	Does your board regularly review your organisation's data security risk?	Risk is managed through a measured agreed risk process at NHSBT, in line with the Board assurance framework. NHSBT is also certified to the ISO22301:2013 Business Continuity Standard.
2	Does the most senior member of your organisation responsible for Information Risk (Senior Information Risk Owner) attend your Board?	Aaron Powell, Chief Digital Officer attends the Board, and holds the dual roles of SIRO and DPO.
3	Has your Board been trained on data/cyber security matters and the things they should be considering and scrutinising in relation to cyber?	NHSBT Board receives regular briefings on cyber security from internal and external bodies. The Board regularly queries issues it has seen in the news etc, demonstrating high awareness and commitment to the cyber security agenda. A number of NEDs have attended seminars at the DH in relation to cyber security.
4	Does your organisation's assurance and risk committee have access to the skills necessary to assist the Board on the management of data/cyber security and information risk?	The Governance and Audit Committee serves this function for NHSBT and has representation from all areas of NHSBT. The GAC works to the Board assurance framework and also receives reports from our internal audit provider in respect of cyber security matters.
5	Is your organisation compliant with the 2017/18 Data Security and Protection Requirements?	NHSBT is compliant with the majority of requirements and is actively engaged on the small improvement activities required to achieve full compliance. The requirements are largely those identified in this table, along with the GDPR programme to which NHSBT is committed.
6	Does your board have oversight of how well the organisation is responding to CareCERT alerts (warnings from NHS Digital about potential cyber vulnerabilities) and whether action is being taken within required timescales?	Reporting is compiled to illustrate the compliance level for CareCERT alerts. Alerts are circulated to the key operational teams and the Head of Information Security to assess whether action is required. Quarterly meetings are held to review whether there is evidence of any emerging threats. The Executive Team has a standing agenda item to be made aware of any information governance and security incidents.
7	Is your organisation aware of the other information security services available from CareCERT?	NHSBT staff, in particular the Chief Digital Officer, Head of Information Security, and Assistant Director, IT Services and Operations, are aware of the breadth of services offered by CareCERT.
8	Has your organisation put its staff through the new data security and protection e-learning?	This element is a gap which is being addressed. All NHSBT staff receive in-house mandatory training, and this requirement will be added to the requirements.

9	The General Data Protection Regulation (GDPR) and (for those organisations in scope) the Network and Information Systems Directive (NIS Directive) will come into force in May 2018. Together, these will strengthen the cyber security and data protection regulatory regime for health and care organisations, and the penalties for breaches. Is your organisation ready?	Both a NIS Compliance and a GDPR compliance programme are underway. NHSBT will continue to work towards full compliance.
10	Has your organisation undertaken an independent on-site assessment (organised through NHS Digital), to identify potential vulnerabilities? If it has, have the findings been acted upon?	NHS Digital are aware of NHSBT's independent security stance and supportive of it. NHS Digital agrees that the on-site assessment is not appropriate for NHSBT.
11	Does your organisation have a plan in place to remove, replace or actively mitigate or manage the risks associated with unsupported systems?	There is a programme to 1. identify and manage out legacy and unsupported equipment. 2. ensure mitigations are compliant with Best Practice This leverages a risk-based approach to protecting the wider environment.
12	How is your organisation planning to transition away from Windows 7 ahead of it becoming unsupported in January 2020?	Windows 7 (and earlier versions) are being replaced as a user desktop by Windows 10 and Windows Server 2016.
13	Has your organisation signed up with NHS Digital for Microsoft Enterprise Threat Detection? This service improves threat awareness, is free to NHS organisations and only takes 15 minutes to set up. Contact NHS Digital for more information.	The Microsoft Service is being evaluated against the current controls and countermeasures in place to determine how and if it can harden NHSBT's security posture. A plan has been developed to implement Threat Detection by May 2018. The comment in the letter about only requiring 15 minutes to set up is misleading as the software has the potential to cause network bandwidth and other performance issues and therefore requires proper review before implementation.
14	Do your organisation’s business continuity and disaster recovery plans cover cyber incidents? When were they last exercised?	Yes. The organisation is accredited to ISO22301 Business Continuity. It has mature processes which are applied to all incidents, and not just cyber incidents. Annual checks are made, and a full BC exercise is scheduled for the coming months.