Trust Board Meeting
01 June 2017

Title of the paper	**Cyber security incident briefing**
Agenda item	**12/49**
Lead Executive	**Lisa Emery, Chief Information Officer**
Author	**Lisa Emery, Chief Information Officer**
Executive summary **(including resource implications)**	The purpose of this paper is to provide a briefing to the Board regarding the Trust's response to the recent international cyber security incident
Where the report has been previously discussed, i.e. Committee/Group	Finance and Investment Committee

Action required:

- The Board is asked to note the report for information

Link to Board Assurance Framework (BAF)	*[Please indicate which Principal Risk this paper relates to by double clicking on the corresponding box]* ☒ **PR1** Failure to provide safe, effective, high quality care ☐ **PR2** Failure to recruit to full establishments, retain and engage workforce ☐ **PR3** Current estate and infrastructure compromises the ability to deliver safe, responsive and efficient patient care ☒ **PR4a** Underdeveloped informatics infrastructure compromises ability to deliver safe, responsive and efficient patient care – IM&T ☐ **PR4b** Underdeveloped informatics infrastructure compromises ability to deliver safe, responsive and efficient patient care – Information and information governance ☐ **PR5a** Inability to deliver and maintain performance standards for Emergency Care ☐ **PR5b** Inability to deliver and maintain performance standards for Planned Care (including RTT, diagnostics and cancer) ☐ **PR7a** Failure to achieve financial targets, maintain financial control and realise and sustain benefits from CIP and Efficiency programmes ☐ **PR7b** Failure to secure sufficient capital, delaying needed improvements in the patient environment, securing a healthy and safe infrastructure ☐ **PR8** Failure to engage effectively with our patients, their families, local residents and partner organisations compromises the organisation's

	strategic position and reputation. ☐ **PR9** Failure to deliver a long term strategy for the delivery of high quality, sustainable care ☐ **PR10** System pressures adversely impact on the delivery of the Trust's aims and objectives PR6 – business continuity has been closed (incorporated into PR1)
Trust objectives	*[Double click on the box to mark as appropriate]* ☒ To deliver the best quality care for our patients ☐ To be a great place to work and learn ☐ To improve our finances ☐ To develop a strategy for the future
Benefits to patients/staff from this project/initiatives Mitigation of risk of cyber attack and impact on access to clinical systems and information	
Risks attached to this project/initiatives and how these will be managed Risk is managed through the Trust's ICT departmental governance, with assurance through the Finance and Investment Committee	

Agenda Item: 12/49

Trust Board Meeting - 01 June 2017

Cyber Security Incident Briefing

Presented by: Lisa Emery, Chief Information Officer

1. Purpose

1.1 The purpose of this paper is to provide a briefing to the Board regarding the Trust's response to the recent international cyber security incident.

2. Background

2.1 On Friday 12th May 2017, a number of NHS organisations were affected by a ransomware attack (an attack on the IT systems which support NHS services). This attack was not specifically targeted at the NHS but it had an impact on NHS services. West Hertfordshire Hospitals NHS Trust was not directly affected by the cyber attack, however did take steps to mitigate the risk of an attack.

2.2 The Trust has already taken steps to reduce the risks posed by cyber attacks. In November 2016, the Trust became an early adopter of the CareCERT service provided through NHS Digital. CareCERT is a national service providing expert advice and guidance on cyber security threats and best practice to the NHS and other health and care organisations. CareCERT (Care Computing Emergency Response Team) is run by experts at the Health and Social Care Information Centre and aims to enhance cyber resilience across the health and social care system.

2.3 The Trust ICT team has taken recommendations from CareCERT regarding actions required to improve cyber resilience. These actions have included undertaking security penetration tests (note these were also undertake prior to joining CareCERT). CareCERT recommendations have been shared with the Trust's ICT suppliers and action plans are in place to deliver on these. These actions will be monitored through weekly executive level governance meetings.

3. Analysis/Discussion

3.1 Below for information is a brief timeline of events and actions taken by the Trust.

Friday 12th May

- At approximately 13.00, the Trust experienced a general network issue which caused problems with access to some clinical applications. This incident was logged as a high priority, and working with ICT suppliers was managed to successful closure at approximately 15.30. This incident was *not* related to the international cyber attack reported the same day.

- During the afternoon, reports came in to the Trust of the ransomware attack affecting a number of organisations.
- At 15.30 a critical incident communication was sent out to incident responders in the Trust.
- At 15.45 a recommendation was made by the ICT team to the Trust Executive to close down all external links in to the Trust and to focus resource on updating and patching end user devices (c. 3,000) and servers (c. 350) to levels recommended by NHS Digital. This was following an internal risk assessment which took into account:
    - Available information regarding the cyber threat
    - The Trust's current infrastructure estate
    - Information held by the Trust regarding CareCERT recommendations
    - Operational impact to the Trust
- At 16.00, external links were closed down. Briefings were issued to staff through the Emergency Resilience and Planning team.
- NHS England declared the cyber attack as a major incident, and reporting systems were put in place for Trusts to provide regular briefings.

Saturday 13th/Sunday 14th May

- Server and end user devices updated and patched
- Some key external links reconnected (following risk assessment)

Monday 15th May

- Server and end user devices updated and patched
- Internal email restored

Tuesday 16th May

- Server and end user devices updated and patched
- Further external key links restored

Wednesday 17th May

- Server and end user devices updated and patched
- All remaining external key links restored

Thursday 18th May

- Server and end user devices updated and patched

Friday 19th May

- Any residual unpatched devices removed from Trust network
- Confirmation of status provided to NHS England

3.2 During the timeframe reported above, disruption to patient services was minimal as access to core clinical systems was preserved, and where required business continuity procedures were followed.

3.3 The Trust ICT team continues to review and implement the recommendations from CareCERT as described in 2.3 above, in order to mitigate risks posed by future cyber attacks.

4. Recommendation

4.1 The Board is asked to **note the report for information and assurance.**

Lisa Emery
Chief Information Officer

24 May 2017