NATIONAL QUALITY BOARD

For meeting on: 06 September 2016

Paper presenter: Will Smart, Chief Information Officer for Health and Social Care, NHS England
Paper author(s): Paul Fleming, Regional Head of Digital Technology, NHS England (Midlands and East)

Paper for:

Decision	Discussion	Information
	X	X

DIGITAL TECHNOLOGY 'WANNACRY' CYBER INCIDENT UPDATE

SUMMARY

This paper provides the National Quality Board (NQB) with an update on activity in the aftermath of the 'Wannacry' ransomware cyber incident of May 12th. It also provides an opportunity for the NQB to discuss and consider the clinical impact of, and clinical learning from, such incidents.

PURPOSE

The NQB is asked to:

1) **Note** the headline figures regarding impact of the 'Wannacry' ransomware cyber incident;

2) **Note** the ongoing activity and challenges around Cyber and the planned investment in Cyber resilience;

3) **Discuss** the key learning that needs to be taken on board by clinicians now, e.g. to prevent a future cyber incident and limit the clinical impact following a potential successful cyber incident; and

4) **Consider** the potential role of the clinician and the clinical informatician in the future.

ALB Involvement in development and sign-off of paper:

NHS England	Care Quality Commission	NHS Improvement	NHS Health Education England
X			

Public Health England	NICE National Institute for Health and Care Excellence	NHS Digital	Department of Health

DIGITAL TECHNOLOGY 'WANNACRY' CYBER INCIDENT UPDATE

Report of Paul Fleming, Regional Head of Digital Technology

1 PURPOSE

1.1 To provide the National Quality Board with an update on activity in the aftermath of the 'Wannacry' ransomware cyber incident of May 12th.

2 BACKGROUND

2.1 The international Cyber incident of May 12th 2017 affected NHS providers across parts of the NHS system. The incident response was led by the EPRR team both nationally and regionally with incident rooms set up across regional offices. The Digital Technology function worked closely with regional and DCO teams as well as care providers and CSUs as part of the incident, until formal closedown.

2.2 The ransomware attacked vulnerabilities in unpatched Microsoft computer systems and propagated across NHS computer networks. Affected organisations were required to remove computers from the network, initiate a nationally prescribed remedy and patching process before re-joining computers to NHS networks for safe use.

2.3 In addition to receiving assurance of incident resolution within organisations NHS England also received assurance from CCGs and Providers around the patching of Microsoft computer systems and Anti-Virus software.

2.4 Lessons learned activities have taken place across EPRR and Digital Technology functions. Much of the early lessons have highlighted a requirement for better communications across the system and better cyber resilience within organisations.

2.5 A national response report has been commissioned by the Department of Health and is being led by the NHS Chief Information Officer Will Smart. This report will be completed in November. The National Audit Office and National Cyber Security Centre will also publish reports later this year.

2.6 The response report will focus on the internal audits and lessons learned of local organisations, national and regional lessons learned from NHS England and NHS Digital teams as well as the future in relation to standards and leadership.

2.7 A detailed review of the clinical impact of the incident is not part of the scope of the CIO report into Wannacry. The report will however reference any information that is already available around service and clinical impact as context to the wider technical issues and response.

2.8 The NHS Digital Care Cert service is commissioned nationally to lead on cyber security across the NHS and publishes regular advisory notices for organisations nation-wide. These advisories are rated low to high, with 'high' Care Cert advisories aimed at tackling critical vulnerabilities in NHS systems.

3 HEADLINE FIGURES REGARDING IMPACT

3.1 47 organisations were infected with Wannacry (27 acute and 20 non-acute). 1,220 diagnostic devices were infected (1%). 595 GP practices were infected (8%). This resulted in:

- 438 cancelled inpatient procedures
- 1,121 day case cancellations
- 6,102 first outpatient cancellations
- 223 two-week wait cancellations

4 OVERVIEW OF ONGOING ISSUES AND ACTIVITY AROUND THE CIO REVIEW

4.1 Since the incident in May a small number of residual incidences of the Wannacry ransomware remain across organisations in England. Typically these issues involve single computers or third party managed computer equipment.

4.2 NHS Digital Care Cert notifies organisations directly by email notification if they are affected by a Cyber threat. This includes residual issues with Wannacry.

4.3 A team has been established to produce the CIO review into Wannacry, using existing resources from across the NHS and DH.

4.4 Provider and Commissioners were asked to provide the CIO review team with their local lessons learned in the form of formal reports, board papers and internal documents. Documents have now been received from a large number of organisations and analysis will take place throughout September.

5 NEXT STEPS

5.1 Care Cert is due to implement an automated, self-service portal for organisations to provide future assurance to NHS Digital and NHS England. A date for the implementation was not available at the time of writing.

5.2 A national investment fund of £21m has been agreed and announced to support Cyber resilience for Major Trauma Centres and Ambulance Services. Organisations have been contacted by NHS Digital as part of a review into requirements before funding is released.

6 RECOMMENDATIONS

NQB is asked to note the ongoing activity and challenges around Cyber and the planned investment in Cyber resilience.

Paul Fleming
Regional Head of Digital Technology (Midlands & East)
30/08/2017