Greater Nottingham Clinical Commissioning Groups

Lessons Learned from the Cyber Attack of 12 May 2017

Introduction

1. On Friday 12 May 2017 the CCG and GP Practices were notified by the Nottinghamshire Health Informatics Service (NHIS) that the NHS had been attacked by ransomware.

2. This cyber security attack was seen worldwide and had a significant impact across many countries.

3. The purpose of this report is to summarise the key events that occurred due to the WannaCry Ransomware attack that hit the Greater Nottingham CCGs, and their respective GP Practices, and describe the lessons learnt from these events. It also sets out the subsequent actions planned to mitigate the risk of future attacks and provides additional assurance in relation to cyber security.

4. The vocabulary used in the report has been modified to help the non-technical reader and in doing so has simplified the nature of the incident and the corresponding response. The reader, therefore, is asked to be cognisant of this fact when seeking any further assurances.

5. A more detailed report will be considered at the CCGs' IGM&T Committee in September 2017.

Background

6. The provision of IT services and infrastructure to GP Practices and CCGs is delivered by the Nottinghamshire Health Informatics Services. NHIS also provide these services to Sherwood Forest Hospitals FT, CityCare and a number of smaller NHS-related organisations.

7. As the report will show, despite the loss of IT services, clinical services remained available to patients at all times throughout the cyber-attack and the subsequent recovery phases.

8. At no point, during or after the cyber attack, was patient information compromised.

Anatomy and Chronology of the WannaCry Attack

9. A summary of the chronology of the WannaCry attack is shown as Appendix A to this report.

10. Critical time scales were as follows:

Event	Date and Time	Elapsed Time
Cyber attack suspected	Friday 12 May, 11:56	-
All systems shutdown	Friday 12 May, 14:41	2 hrs 45 mins
Out-of-hours services re-established	Saturday 13 May, 01:14	13 hrs
CCG Control Room established	Saturday 13 May, 08:00	20 hrs

Event	Date and Time	Elapsed Time
Clinical systems accessible to all GP Practices	Tuesday 16 May	4 days
Patching complete	Friday 19 May	7 days
CCG Control Room stood down	Tuesday 23 May, 17:00	11 days
All infected machines recovered	Friday 26 May	14 days

11. Importantly during the initial phase of the attack NHIS shutdown the network and IT services to prevent further cross infections between sites.

12. In recovering the IT services the CCG and NHIS took a low risk approach to ensure any cross infection was minimised. This required the confirmation of clean machines on each site prior to reconnection to the wider network. Whilst this prevented further infections it did inhibit a faster re-establishment of services, particularly at sites with some degree of infection.

13. The CCG's responsibilities across the wider health community required some direction of the NHIS resources and their capacity to recover clinical services at other providers, in particular Sherwood Forest Hospitals FT and the GP out-of-hours service provided by NEMS.

14. In some respect the attack taking place on a Friday was less disruptive than at other times of the week. The emphasis over the weekend of 13/14 May was prioritised on 24-hours services, meaning recovery of GP services was attended to from Sunday 14 May.

15. Throughout the attack the CCGs' Incident Control Room was chaired by an Accountable Officer and had permanent membership from the EPRR Lead, On-Call Manager, Director of Outcomes & Information and a loggist. Other members of the team were drawn into the Control Room at appropriate times so that a cross-CCG membership was maintained to provide local knowledge at a CCG and Practice level.

16. To support the rapid recovery of systems CCG staff were deployed to GP Practices to support NHIS staff in patching the individual PCs. The NHIS control room coordinated the movement of staff with direction on priority being taken from the CCG control room. The prioritisation of GP Practice sites was based on a number of factors, including:
    a. Whether the Practice had any uninfected machines available from which to access their clinical system;
    b. The number and proportion of infected machines on each site;
    c. The provision of any alternative IT equipment on the site;
    d. The size of population being covered by the Practice / site;
    e. Whether the GP Practice had access to alternative methods of accessing their clinical system; and
    f. The physical location of the site.

17. The key consideration during this part of the recovery was to ensure all Practices had a minimum number of machines to access their clinical systems. The chronology states all Practices were fully operational by Tuesday 16 May but it should be acknowledged that many Practices were operational on the Monday 15 May.

18. Throughout the attack information was provided to NHS England on the status of each Practice and the availability of clinical services.

Impact on Nottinghamshire Health Community

19. The overall impact to the organisations in the Nottinghamshire health community was light, although it is recognised there was considerable variation in the level of infection at different locations.

20. As already discussed, the initial isolation phase inherently required the temporary loss of remote IT services and this was disruptive to most organisations irrespective of whether local infection had taken place.

21. Following the cyber-attack, the investigation carried out did not reveal any intelligence surrounding the reasons for the variation across the Nottinghamshire geography. There was a higher level of infection in the southern part of the patch than in the northern part. However, investigations proved inconclusive in determining the exact cause of the variation, the presentation of the index case, nor why the cross infection appeared to be higher in the south.

22. NHIS continue to liaise with the National Cyber Crime Unit (NCCU) as part of the wider, national criminal investigations.

Lessons Learned

23. Whilst the impact across west Nottinghamshire was, on this occasion, reasonably light, there are still a number of lessons that GP Practices, the CCG and NHIS can learn from the attack.

24. The CCGs have undertaken a comprehensive assessment of the cyber attack including sessions with its staff and GP Practices in hearing feedback on positive and negative aspects of the events. These have been documented and used to consider necessary actions.

25. Similarly, NHIS have undertaken a technical investigation and the full version of this report has been shared with the CCGs.

26. NHS England has run a cyber-attack formal review and debrief attended by EPRR leads from across the North Midlands. The findings of this will be published in due course.

27. The CCG has identified lessons in the following categories:
    a. Technical
    b. Communications
    c. Business continuity

<u>Technical</u>

28. The CCG had maintained a PC refresh programme that meant that the vast majority of workstations were running Windows 7, a supported operating system. This minimised the risk of infection, it is recommended that the CCG should work with NHIS to maintain this position.

29. The status of Operating System upgrades and patches applied across the estate was unclear due to the complexity of the network and the lack of up-to-date information through the suite of management tools in use at the time of the cyber-attack.

30. Each machine had antivirus software loaded, however, the anti-virus signature file updates had not been applied consistently to each machine.

31. Perimeter security on the Nottinghamshire community of interest network (COIN) seems to have been inconsistent due to the partial migration from the "old" COIN to the newly commissioned service.

32. A number of file servers and peripheral devices in GP Practices were shown to have the Operating System vulnerability. Some of these devices are not the formal responsibility of NHIS. The CCG should work with NHIS to document the existence of these devices and implement a robust asset management process.

33. A summary of the recommendations made to the IGM&T Committee is as follows:

Recommendations

1) Rigorous patching regime needs to be agreed with NHIS, with greater focus on enforcement over disruption i.e. forced reboots.
2) Regular IT health checks to take place to catch vulnerabilities / protection / remediation.
3) Vulnerability testing to be conducted on a regular basis by NHIS not just via audit processes.
4) Investigate what additional resources NHIS may need to prevent future attacks.
5) Version Control Sign-off of patches and changes at NHIS senior level and single point of contact to ensure accuracy and consistency of changes across the whole estate.
6) NHIS to ensure speedy completion of the COIN migration to minimise the risk of future limited remote device management.
7) NHIS to implement a robust process for IT asset management.

Communications

34. Key communications routes through email, internal file & print services and the internet were disrupted when the network was disabled to minimise the potential spread of the ransomware.

35. Updates from NHIS for GP Practices were actioned through the CCG leads, which resulted in mixed messages and delay in receipt of information to and from the NHIS operations and project management hub.

36. GPs who had remote access continued to try to use systems over weekend and into the week.

37. There was not a readily available emergency contact number for all GP Practices over the weekend.

38. Contact numbers were often held electronically and were therefore inaccessible.

39. The central person in each CCG worked well.

40. A summary of the recommendations made to the IGM&T Committee is as follows:

Recommendations

8) Text facility for CCG staff, NHIS staff and GP Practices to be set up to facilitate emergency communications.
9) Investigation of use of alternative technology for communication via internet based services (i.e. a WhatsApp group, Facebook, etc.).
10) BAT phone utilised (i.e. a private telephone number that is handled at a higher priority).
11) Key contacts / communications lead to attend NHIS control room for communications updates and ensure all disseminated messages are consistent.
12) Cascading communication system to be agreed which would also prevent multiple people contacting CCG and NHIS staff for the same queries. Dedicated NHIS and GP Practice liaison leads.
13) Shared off-duty / emergency contacts across the health community.
14) Each GP to have an emergency mobile contact number that is accessible out of hours.
15) Central list to be held in a format and location that can be accessed if the systems are down.
16) On-call to have details of how to access all contact details.

Governance / Business Continuity

41. Business continuity plans were appropriately executed during the cyber-attack taking into consideration the time of day and the level of information known.

42. After the cyber-attack (the evening of Friday 12 May onwards), elements of the business continuity plans were executed. However, the actions outlined for this type of event relate to working from a different base which was not possible.

43. Over the weekend it was possible to coordinate a system-wide view of the impact and this was supported through the NHSE Tactical Coordinating Group (TCG). The scale of the impact (infected and affected) on primary care and other clients (i.e. CityCare) was not fully understood by NHIS impacting on the understanding of the system wide view and the availability of clinical service

44. Although all organisations demonstrated that business continuity plans were in place and could action these to some extent, response to a major incident had not been tested across the local health community and involving multiple agencies.

45. Current plans have worked well in the past but need revising for a larger scale major incident. This also needs to be rehearsed and tested.

46. There is a need for the creation and maintenance of major incident resources available off-line, holding paper key information, such as customer contacts, staff contact numbers should all electronic sources be unavailable – and these need to be updated regularly.

47. Although all agencies worked together with regular meetings and updates, there were conflicting priorities for resources and deployment of technical teams to bring services online.

48. A summary of the recommendations made to the IGM&T Committee is as follows:

Recommendations

17) Commission an external audit of the cyber security arrangements in place across the CCGs and within NHIS, ensuring the commissioner has systems in place to test this on an on-going basis.
18) Consider the use of a single incident room to be used for all organisations. Priorities agreed across the health community based on patient risk. This would significantly reduce the number of meetings and conference calls needing to be attended.
19) Business Continuity Plan to reconsider critical functions, definition of and min/max times of disruption.
20) To include in the Business Continuity Plan contingencies for no IT across the system.
21) To include in Business Continuity Plan more detail on systems impacts i.e. if "*x*" is down then "*y*" is not available and use "*z*" as contingency.
22) To review other areas in business continuity relevant to lessons learnt from cyber-attack incident.
23) Establish working group to review and establish system-wide GP Practice Business Continuity Plans including critical functions, asset registers, emergency contact details, relevant contingencies. Include a list of what Practices should have in stock to operate a paper based system i.e. appointments, FP10, blank "acute" templates.
24) CCGs to have conference call facilities that are not linked to MITEL phones.
25) Cupboard for emergency planning including a Pay-As-You-Go SIM, contact numbers – staff / member Practices / system-wide partners / emergency services, business continuity plan, EPRR handbook.
26) Investigate the use of "One Drive" or other external storage systems for major incident Plans and other key information such as site lists, etc.
27) Review NHIS SLA to set a threshold of capacity for NHIS, i.e. in order to mobilise CCG staff more effectively when NHIS is up to capacity.
28) Ensure expenses protocol agreed as necessary in order to support recovery.
29) CCG on call staff to have mandatory training in running a TCG. CCG to have trained loggists.
30) List of stakeholders / partners and how can use as part of recovery depending on what systems / providers impacted (i.e. how can community pharmacies be used to support).
31) Mapping in incident recovery / business continuity plans to provide non-IT people with an understanding of what and how clinical services will be impacted i.e. ICE, e-referrals, diagnostics and what contingencies are available or how to implement the contingencies.
32) Review the role of the IGM&T Committee to ensure there is a greater level of assurance on the policies supporting cyber security and the robustness of the tactical and operational processes being undertaken by NHIS to deliver these.
33) Commission an external audit of the cyber security arrangements in place across the CCGs and within NHIS, ensuring the commissioner has systems in place to test this on an on-going basis.

Next Steps

49. The continued focus on cyber security is paramount. The CCG, NHIS and GP Practices should work on the assumption that another attack will hit the NHS at some point in the future.

50. The cyber assurance report presented to the Audit Committees in March 2017 and IGM&T Committee in June 2017 identified a number of safeguards in place across the Nottinghamshire IT estate which mitigated cyber risk. It is clear from the event on 12 May these risks need to be reviewed and further mitigations considered.

51. Many of the thirty three recommendations made in this report have already been actioned and in some areas completed, reducing the residual risks. The remaining recommendations should be actioned and their progress monitored through the appropriate governance structure.

52. Specifically, the consideration and satisfactory completion of the technical aspects should largely be monitored through the CCGs' IGM&T Committee, the communications, governance and business continuity recommendations should similarly be monitored through the CCGs' EPRR Working Group. This will include the production of an initial, detailed action plan, the progress against which will be reported to the CCG Governing Body.

53. It should be noted there is not a strict categorisation of the recommendation and which of these two fora should progress them. The IGM&T Committee, for example, has already considered the policy review. However, the two fora must work together to ensure all recommendations in this report are considered.

Recommendations

54. The Governing Body is asked to:
    a. **ACKNOWLEDGE** the content of the Report and the current update on the cyber attack of 12 May 2017;
    b. **ACKNOWLEDGE** the recommendations for further actions to mitigate the risks of future cyber attacks;
    c. **ACKNOWLEDGE** that some of the actions have already been completed;
    d. **APPROVE** the recommendations and request action plans to be drawn up; and
    e. **NOTE** regular reports on the progress of the actions will be presented to future meetings of the IGM&T Committee.

Andy Hall
SIRO and Director of Outcomes & Information
11 September 2017

Appendix A – Summary Chronology

Date	Time	Event
Friday 12 May	11:56 – 12:04	Reports of ransomware infection on two sites reported to NHIS
	12:30	NHIS report cyber attack reported to CCGs
	14:30	NHIS seek external specialist support
	14:41	All network shutdowns completed by NHIS as precaution
	14:54	Cyber attack confirmed as a global event
Saturday 13 May	01:14	NEMS out-of-hours SystmOne re-established
	04:00	SystmOne connectivity re-established
	08:00	CCG Control Room established virtually
	10:25	CCGs confirm initial list of infected machines in GP Practices
Sunday 14 May	08:00	CCG Control Room relocated to Lings Bar Hospital
	16:45	Confirmation that first GP Practice successfully patched
	17:00	Further infections seen at un-patched sites
	17:00 – 21:00	Business Continuity plans in place within CCGs and Practices
Monday 15 May	15:30	NHIS deploy engineers to manually patch machines
Tuesday 16 May	09:45	CCG staff deployed to support manual patching
	10:00	Network connectivity restored to GP Practices
		All GP Practices able to access clinical system
Wednesday 17 May		CCG HQ buildings operational
Thursday 18 May		Laptop clinics established
Friday 19 May		Patching largely complete
Monday 22 May		External systems operational for GP Practices, e.g. ICE and eRS
Tuesday 23 May		CCG Control Room stood down
Friday 26 May		New VPN solution in place
		Recovery of infected machines complete