B/17/74

NSS Formal Board Meeting – Thursday, 29 June 2017

NHS Scotland Cyber Attack: NSS Evidence to Scottish Parliament Health & Sport Committee (Jun 17)

Purpose

The Board is asked to review and consider written evidence supplied to the Scottish Parliament Health & Sport Committee by NSS IT Director in wake of Wannacry cyber-attack on NHS Scotland IT estate in May 17.

Recommendation

The Board is asked to note the evidence supplied and invited to ask questions around the role of NSS IT in the handling of the attack and in the subsequent recovery / analysis of events and lessons learned. The Board is asked to make recommendations on any follow up required.

Timing

There are no particular timing considerations in this matter but the Board may wish to recommend appropriate actions and timelines around any follow up activity agreed.

Background

On Friday 12th May 2017 the Wannacry malware spread across global IT networks and the incident was widely covered in UK press. The malware encrypted local files and demanded a ransom for the files to be restored to normal ("ransomware") and also spread via the network using exploits against Windows operating systems. NHS Scotland experienced some impact from this malware.

NSS at the Board level was only minimally impacted. However, the NSS IT organisation was heavily involved in the coordinated NHS wide response to the incident and the NSS Director of IT volunteered to serve as a witness at the Scottish Parliament Health & Sport Committee held at Holyrood on June 20. The paper supplied was submitted as written evidence in advance of the Committee meeting.

Engagement

A sub-group of the NSS Exec Mgt team have provided advice, guidance and challenge to the Director of IT in preparation for the Parliament Committee session. The same core paper was presented to the NSS Audit & Risk Committee on Thursday 22 June 2017.

Name of the Author : Andy Robertson
Designation : Director of IT
Tel: 0131-275-6689
Email: andy.robertson@nhs.net

Health & Sport Committee: 20 June 2017: Witness Written Evidence

Andy Robertson, Director of IT, NHS National Services Scotland (NSS)

Introduction & Context:

The NSS IT organisation provides a range of national level IT services to NHS Scotland Boards including the hosting and management of the role of the National IT Security Advisor. This position involves heavy collaboration with other Boards and provides a consulting and coordination role on IT security issues across the NHS in Scotland. We link into Scottish Government and UK level policy on IT security matters, and provide practical guidance and frameworks for the assessment of local measures put in place to mitigate different types of threat. In the event of an incident, we act as a coordinator and clearing house for information sharing and provide central guidance back out to Boards on how best to deal with issues in real time. We link into all the national public sector support available (Cyber Security agencies within Scotland and the UK) and provide coordinated status information back to Boards and into Scottish Government eHealth directorate. We also provide recommendations on recovery and on any changes which need to be made to counter any repeated incidence and ensure delivery of incident reviews and lessons learned exercises. We also link into national level IT service suppliers on security issues and provide contract guidance on security aspects of all major IT purchases across NHS Scotland.

I have listed below answers to key questions posed by the Committee to all NHS Boards….

1. What impact did the recent cyber-attack have on your organisation and the public?

NHS Scotland is comprised of 22 separate health Boards that provide regional health services (e.g. NHS Lothian, NHS Lanarkshire, etc.) and national functions (e.g. Scottish Ambulance Service, National Services Scotland, etc.) across the whole of Scotland. This answer provides an overview of the impact across all of these separate organisations.

On 12 May there was a global Ransom ware attack that impacted on a number of countries but in the UK mainly affected the NHS. Across Health Boards around 1% of the total number of devices (around 1,500 devices) were affected by this cyber-attack. Mainly Windows 7 and small number of Windows XP devices were affected along with a number of Windows 2003 servers. Initial consideration suggests that the source of the attack was not through an infected email or a click-through to a malicious website. Rather it appears to have been through an open end port (which provides the 'gate' onto other networks internal to NHS and externally, including the internet and the NHS England network) and through which the Ransom ware found its way in. Once inside our networks the Ransom ware was then able to encrypt files it got access to and jump from one network connection to another thus spreading quickly to vulnerable computers.

Impact varied across NHS Scotland as health boards were affected differently. In total, 11 territorial Boards and 2 national Boards were affected.

- **No infection**: Nine of Scotland health boards were not infected by the malware
- **Minor infection**: Several health boards experienced mild infection in the order of 2-10 devices infected. The impact of this was typically minor including overtime resource to

restore infected servers and endpoints and GPs and some business areas reverting to business continuity processes whilst services were restored. In most/all cases normal service was restored in the following 24 hours

- **Wider infection**: Two health boards experienced a more significant impact including 30+ devices infected across multiple sites, more disruption to normal business and in some cases rescheduling of non urgent appointments

There was also a limited impact on national level systems:

- **Scottish Wide Area Network (SWAN):** Restrictions on network traffic were put in place to restrict virus propagation soon after the attack started. This did have temporary impact on legitimate network traffic which did delay some of the usual information flows but these connections were restored once the attack risk had been mitigated. No significant impact on operations were reported linked to this measure.
- **Finance Systems**: One module of the national financial systems suite was impacted by the virus and this did drive the need to shut down access to core national financial systems into the start of the new working week whilst the impacted module was cleansed. The recovery measures worked as planned and there was no impact from a data integrity perspective. Full access was restored by Tuesday 16 May.
- **Digital Imaging System (PACS)**: The national PACS data archive was taken down as a precautionary measure but was found not to be infected. This necessitated business continuity measures to be put in place for urgent cross Board access to x-rays and scans over the attack weekend with no reported impact on service provision to the public.

Notes on impact of the incident:

- **Service restoration**: across the whole of NHS Scotland the majority of critical services were restored in less than 24 hours, and full normal service resumed less than a week later
- **No ransom paid**: no health board paid any ransom because of extensive data restoration capability, so systems and data were restored from backups where required
- **Impact on resource**: probably the biggest impact to NHS Scotland resource was the additional demands placed on IT teams, and the disruption of business as usual activities displaced by re-allocation of resources to investigate and respond to the incident
- **Precautionary measures caused disruption**: some health boards, even with no infection, took the decision to shut down systems or disconnect networks as a precautionary measure – this can be an effective approach to prevent a system being infected and limit the potential impact, particularly early during an incident when the method of infection is yet to be confirmed, but also can cause self-inflicted business impact and disruption so a careful consideration is required

2. Following the cyber-attack how has your approach to prevention of such attacks been revised?

NHSScotland's national approach is to implement the SG eHealth NHS Scotland Information Security Policy Framework (NHSS SPF). This is a national framework of security objectives derived from industry good practice standards ISO27001 and ISO27002 that builds on the previous national information security policy and was mandated to all health boards from Scottish Government in July 2015.

At health board level this entails implementation of health board security policy, standards and local good practice to meet the control objectives. To achieve this health boards draw on multiple resources and supporting industry good practice such as National Cyber Security Centre guides, Top 20 Critical Security Controls and independent audits.

Overall health boards implement extensive security good practice, however, all organisations are restrained by budget and available resources and must make decisions to balance risk vs. expenditure when mitigating security risks and the NHS is no exception.

- The scale and complexity of the NHS, and particularly NHS supplier arrangements, can present a challenge in achieving 100% coverage of controls such as patching and upgrading legacy infrastructure with very limited resources
- The NHS typically does not have internal skills and budget to implement innovative leading edge security controls such as advanced end point protection, Security Information and Event Management (SIEM) and Intrusion Prevention Systems (IPS) or other automated solutions for tasks like patch and vulnerability management. In some cases the technology may be affordable in isolation but the challenge is in having the skills and budget to implement and manage the solutions on an ongoing basis.

So whilst the overall approach of NHS Scotland to mitigating cyber threats has not been significantly revised, health have identified multiple options that could provide additional mitigation of cyber risks, these are summarised in the next question.

3. What additional support would assist in preventing such attacks?

Health boards have identified multiple areas for consideration where there may be opportunities for improvement.

National initiatives

- **GP review**: full review and re-alignment of GP security posture, controls and responsibilities e.g. GP governance, infrastructure improvements, training and awareness around cyber security risks/impacts

- **Security training**: covering all areas such as awareness for front line staff, security skills and certification for IT and security personnel and courses targeted at GP surgery managers
- **NHSS Computer Emergency Response Team**: better monitoring and alerting of information security information e.g. threats, vulnerabilities and recommended mitigations (similar to NHS England / Digital CareCERT function)

National – technical (SWAN, NSS, suppliers and third parties)

- **National vulnerability scanning function**: a centralised team that can be deployed to scan national networks such as SWAN, and deployed locally to provide intelligence and reporting on local health board networks
- **SWAN review/network monitoring**: technical solution to provide intelligence, alerting and real-time mitigation of security events at network level
- **Technology standardisation**: development of health board security target model to encourage standardisation, increase efficiency, promote best practice and enable collaborative/national procurement of security technology

Local health board

- **More IT and security skills resource**: managing IT infrastructure to reduce vulnerability requires IT resource. Current resource allocation may be insufficient to keep pace with increasingly rapid development of cyber threats
- **Increased IT budget**: additional funding to enable tech refresh to replace legacy infrastructure and allow the NHS to keep pace with modern technology lifecycles; and/or to deploy more advanced security tools
- **Local technical improvements**: improved patching standards and process, standard build review (reducing/removing unused services); local infrastructure monitoring and control – IPS/SIEM; enhanced endpoint protection; etc.

4. To what extent do you collaborate with other Boards on IT security issues?

Across NHS Scotland and the UK there is extensive collaboration and coordination on security efforts. NSS provides a consulting and coordination role on IT security issues across the NHS in Scotland and NSS also links into Scottish Government and UK level policy on IT security matters.

During the incident there were several instances of collaboration and sharing of information about the malware and action steps to mitigate, including:

- Information shared by one health board, communicated to all others via NSS and the national information security website
- National steps implemented on SWAN to prevent the spread of the malware with extensive communication and collaboration with health boards

- National UK co-ordination via NHS Digital (England) and joint government / industry Cybersecurity Info Sharing Partnership (CiSP) around information and lessons learned
- Communication with Scottish Government to ensure relevant information made available

However, eHealth Leads have recently discussed opportunities to more effectively share good practice of one health board across NHS Scotland. In the eHealth Leads technical workshop (took place several weeks before the incident) an action was agreed to create a health board target security model that would draw on the best practice from each health board.

Table 1 provides a summary of the key NHS Scotland and national UK security groups.

Group	Comment
NHS Scotland	
Information Security Forum (ISF); and Information Governance Forum (IGF)	ISF and IGF are on back to back days and attended by information security and governance practitioners to support sharing of information, reviewing information systems and issues arising and progressing national initiatives
National information security website and discussion tool (https://security.scot.nhs.uk requires N3/SWAN NHS)	Information sharing resource internal to NHS Scotland, similar to National Cyber Security Centre (NCSC) website
Other national groups with security engagement (primarily eHealth Leads and Infrastructure Leads)	Focus of these groups is wider than information security but includes significant focus on security aspects
National – UK	
Home Countries Security Liaison Group (NHS England, Scotland, Wales and NI)	National group of heads of security from each of the home countries health services for sharing information and expertise
NHS Digital CareCERT (Emergency Response Team)	Valuable alerts and information sharing resource
Cyber Information Sharing Partnership (CiSP – online information sharing platform)	Very useful pan UK private and public sector online collaboration and information sharing tool
National Cyber Security Centre (NCSC)	Although the national authority on security, they weren't the first point of contact for information during the recent incident

Table 1: summary of NHSS national and UK group