WANNACRY NO MORE? – CYBER SECURITY IN THE NHS
Introduction

The Wannacry cyber attack created panic within the NHS and the disruption that followed impacted patient appointments, access to health records and the ability to access and use a range of systems.

The longstanding Information Governance Toolkit has provided a framework for NHS organisations to follow when trying to protect patient data. However, the growing sophistication and potency of the recent cyber attacks in the UK and elsewhere in the world has only helped to underline the vulnerability of the NHS. In some ways it can be seen as a soft target, as:

• budget restraints and short term financial decisions have affected the ability of organisations to invest in IT systems and improve their infrastructure;
• public sector pay controls and the competition from the corporate sector have hindered staff recruitment and the ability for NHS organisations to retain some of their best staff; and
• the complex way in which the IT infrastructure has developed in the NHS, involves connecting systems, a plethora of customised applications and a range of unsupported software used in areas such as radiology.

While the recent attack affected only some NHS organisations, it’s a very real warning of what may be to come. The whole sector must now put controls in place to protect themselves from future attacks.

During 2016/17 we undertook internal audit reviews across 44 of our NHS internal audit clients following a Cyber Essentials methodology, and supporting the self-review of each organisation with focused testing. In the following pages we highlight a number of key findings, which focus on the areas of greatest vulnerability where action is most commonly and urgently required.

If you require any further assurance for your organisation or support in building your defences against a cyberattack, please contact us using the contact details on the back cover of this publication or by speaking with your usual RSM contact.

Tim Merritt
Head of Healthcare Sector at RSM
The vulnerability

NHS organisations are failing to embed core security measures and are leaving themselves open to cybercrime. Whilst the security measures vary between organisations, the main weaknesses we have identified can be split into three core themes:

1) Insider attacks – identity and access management

There are no firewall rules or alerts for human carelessness. But, a few basic steps to embedding a security culture can go a long way to mitigating insider misuse. For example, education, training and raising awareness; and ensuring that users access the right resources at the right time and for the right reasons.

- 80% permit network administrative accounts access to the internet or external email
- 50% have a process and policy applied regarding the removal of access for leavers
- 20% document and regularly review elevated / privileges access
- 19% have documented special access privileges and review these regularly

20%
2) External attacks –
patch and software updates

Patch management systems and software updates aim to keep organisations aware of new vulnerabilities that may impact their IT infrastructure. Therefore, a process should be in place to continually monitor, evaluate and classify vulnerabilities.

Classifying risks (by seriousness) allows organisations to identify and address the most severe vulnerabilities quickly. This then reduces the likelihood that they will be exploited.

The recent WannaCry attack highlighted the impact of not implementing up to date patches and updates on key/critical systems and software efficiently. Cybercriminals will exploit this to attack or disable a system or gain access to personal and sensitive data.

- 7% always apply application software security patches within 14 days of their release regardless of vendor risk ratings
- 11% always apply operating system security patches within 14 days of their release
- 50% have software installed on computers and network devices that is unsupported
3) Malware attacks – firewall governance

Firewalls are a key component of the security architecture, essentially blocking insecure or unnecessary services and only allowing permitted websites to be accessed from the organisation’s network. They attempt to ensure that only safe and necessary network services can be accessed from the Internet. It is vital to have a documented and applied process for approving and testing all connections and changes to firewall rules. This will help prevent security problems caused by misconfiguration of the firewall. A documented Firewall Policy should mandate periodic reviews of rules to enable effective cleansing of any unneeded, outdated, or incorrect rules. Failure to do this will leave organisations vulnerable.

21% have a policy to periodically review / disable firewall rules no longer needed
The WannaCry ransomware attack demonstrated that no one is immune from cybercrime and one attack can have wide reaching global implications across all sectors. As public facing organisations hosting critical infrastructure it’s never been more important for the NHS sector to have robust cyber controls and defences in place. Cyber security is an ongoing challenge and whilst you may have an adequate level of protection today, given the rate at which the vulnerabilities are increasing and the continued growth in cybercrime, maintaining an effective and resilient environment of systems and controls to guard against cyber breaches will remain an ongoing challenge for the UK and globally.

Sheila Pancholi
Technology Risk Assurance Partner, RSM
Building your defence

How can NHS organisations protect themselves against continued and evolving cyber threats? As hacker techniques become more sophisticated, no single form of control will provide adequate protection on its own. The NHS sector must instead embed multiple controls and regularly review their position.

**Invest in employee education**

People are key, as network breaches often occur via phishing and social engineering. It is critical for all employees to remain vigilant to suspicious activity and know what role they play in the defence of the organisation (and related services).

At an executive level there needs to be clarity around responsibilities as senior leaders need to guide risk assessment, investment and incident response.

**Review the firewall rulesets every six months as a minimum**

Firewall reviews remove the opportunity for cybercriminals to exploit vulnerabilities from out of date defences. They also ensure that only authorised services and ports can be used on systems.
**Invest in identity and access management (IDAM) solution**

IDAM enables the right users to access the right resources at the right times and for the right reasons.

**Patch systems periodically**

Criminals use security vulnerabilities to gain privileged access to systems. Many of these vulnerabilities can be fixed by vendor-provided security patches.
Overcoming obstacles

NHS organisations need to identify and navigate obstacles quickly and effectively to help protect themselves from future attacks.

1) Budget constraints – limited investment in solutions to automate and simplify security operations

**Potential response**
- A risk-based program, focusing on areas of greatest impact to the organisation.

**What does this mean?**
Risk based approach to cyber security.

Best practice standards (e.g., cyber essentials) are proven to strengthen control frameworks, and assist in preparedness for cyberattacks and other security incidents. Having a risk register enables organisations to formally manage, record and review risks in the context of changing internal and external environments.

2) Financial justification for continued investment in security

**Potential response**
- A direct line between the NHS information security team and senior leadership to have an accurate and realistic view of ongoing cyber threats.

**What does this mean?**
Senior level sponsorship and visibility of threats and challenges.

Senior and executive sponsors should be responsible for cyber security strategy and its effective delivery. As such, they need to be aware of cyber threats and risks to make informed decisions. This includes levels of investment in defences. Sponsors should also be aware of the changing nature of cyber threats. Defences need to evolve in response and as such, the information security manager/lead/team should share regular network security monitoring reports and statistics on threats.
3) Reduce vulnerabilities and educate staff

Potential response
- Sharing cyberattack/threat information amongst sector peers to better detect systemic threats.
- Organisations need to have established and tested plans for responding to cyber incidents such as insider breaches, denial of service attacks and ransomware.
- Effective access control by restricting access to information assets on a need to know and need to have basis.
- Effective network security through the effective management of firewalls, segregation of internal networks, network access controls and other appropriate measures.
- Malware protection by installing anti-virus solutions on all systems, keeping software and browsers up to date and running virus scans daily.
- Establish and test plans for responding to cyber incidents such as insider breaches, denial of service attacks, ransomware.

What does this mean?
Effective preventative and detective controls.
Proactive monitoring could expose security breaches quickly and minimise business disruption, data loss and resulting financial loss and regulatory fines.
Effectively configured network controls decrease the risk of data exfiltration, malware infections, and unauthorised access. This could avoid potentially severe losses of business assets, data, and reputation.
Regular monitoring could include periodic reviews of third party administrative / super-user accounts undertaken to ensure their continued business need is warranted; updates to the existing access control policy to mandate the access reviews of third party users as well.
Defences need to evolve in response and as such the information security manager/lead/team should share regular network security monitoring reports and statistics on threats.

4) Retaining qualified and trained information security staff

Potential response
- Minimising the exposure to critical dependency on key individuals through knowledge capture (documentation), knowledge sharing, succession planning and staff backup.

What does this mean?
Avoiding single points of failure.
Succession planning decreases risk to ongoing business operations, sponsorship and oversight for cyber security. A formal succession plan for key staff roles responsible for cyber security should be developed between Executive Management and Senior Management to ensure ongoing compliance and leadership.

What should all NHS organisations do now?
Dedicate time and resource to assess the condition of cyber defences and introduce effective corresponding controls to address any vulnerabilities.
For more information please contact

Sheila Pancholi  
Technology Risk Assurance Partner  
M +44 (0)7811 361 638  
sheila.pancholi@rsmuk.com

Tim Merritt  
Head of Healthcare  
T +44 (0)1908 687 800  
tim.merritt@rsmuk.com

rsmuk.com

The UK group of companies and LLPs trading as RSM is a member of the RSM network. RSM is the trading name used by the members of the RSM network. Each member of the RSM network is an independent accounting and consulting firm each of which practises in its own right. The RSM network is not itself a separate legal entity of any description in any jurisdiction. The RSM network is administered by RSM International Limited, a company registered in England and Wales (company number 4040598) whose registered office is at 50 Cannon Street, London EC4N 6JJ. The brand and trademark RSM and other intellectual property rights used by members of the network are owned by RSM International Association, an association governed by article 60 et seq of the Civil Code of Switzerland whose seat is in Zug.

RSM Corporate Finance LLP, RSM Restructuring Advisory LLP, RSM Risk Assurance Services LLP, RSM Tax and Advisory Services LLP, RSM UK Audit LLP, RSM UK Consulting LLP, RSM Employer Services Limited, RSM Northern Ireland (UK) Limited and RSM UK Tax and Accounting Limited are not authorised under the Financial Services and Markets Act 2000 but we are able in certain circumstances to offer a limited range of investment services because we are members of the Institute of Chartered Accountants in England and Wales. We can provide these investment services if they are an incidental part of the professional services we have been engaged to provide. RSM Legal LLP is authorised and regulated by the Solicitors Regulation Authority, reference number 626317, to undertake reserved and non-reserved legal activities. It is not authorised under the Financial Services and Markets Act 2000 but is able in certain circumstances to offer a limited range of investment services because it is authorised and regulated by the Solicitors Regulation Authority and may provide investment services if they are an incidental part of the professional services that it has been engaged to provide. Baker Tilly Creditor Services LLP is authorised and regulated by the Financial Conduct Authority for credit-related regulated activities. RSM & Co (UK) Limited is authorised and regulated by the Financial Conduct Authority for credit-related regulated activities. Whilst every effort has been made to ensure accuracy, information contained in this communication may not be comprehensive and recipients should not act upon it without seeking professional advice.

© 2017 RSM UK Group LLP, all rights reserved. 4642