Securing a new lifeline for the NHS

A report by VMware and Intel exploring the evolving cyber threat on the NHS and how it can better protect itself to preserve the security of the UK and its people

Contents

Foreword

The WannaCry ransomware attack hit the NHS hard, affecting as many as 40 hospitals across 24 trusts[1]. It hit services, communications points, and ultimately affected patient care.

WannaCry served as a huge wake-up call for the healthcare industry and for the UK government as a whole. According to guidance from the National Cyber Security Centre[2], an attack of this type and scale could recur.

The subsequent response from the NHS was interesting; while on the whole it managed to protect essential services, different hospitals and NHS trusts handled the attack in different ways – some better than others.

Either way, the attack highlighted how valuable NHS data is to cyber criminals. Whether it's personal data on people or information on ground-breaking research, data is an incredibly important asset in helping to deliver patient care; criminals realise this and are willing to halt services to gain money or aim to sell the data themselves. A communications provider Maintel recently said that "medical information can be worth ten times more than credit card numbers on the deep web"[3].

It is for this reason that strong data security standards are essential for organisations in the healthcare sector.

The importance of such standards is only growing by the day. With the NHS' plans to become paperless by 2020, even more data and services will be available online, increasing the potential for significant data loss. Meanwhile, new data-sharing schemes are continually being proposed and introduced within the public sector as well as between the private sector and the NHS. These projects are designed to improve and extend the services offered by the NHS, satisfying demand for a 24/7 service and providing a more joined-up approach to healthcare to bring greater benefits.

The NHS, constantly[4] ranked amongst the top healthcare systems in the world, has to be able to demonstrate that it can protect this data in order to restore public confidence.

As a result of the WannaCry disruption, the NHS now has the opportunity to lead the way in clinical data security. For the NHS to succeed in delivering world class medical care to any one any where, the public must have complete confidence in the security of their personal information

However it is facing a tough balancing act, having to cope with budget cuts and under-resourced IT teams – all while having to be as resilient as possible in thwarting and reacting to possible cyber threats.

To discover more about how the cyber threat on the NHS is perceived, we questioned IT decision makers (ITDMs) at NHS organisations as well as 2,000 consumers about their experience with and views of cyber security threats – be it external sources, internal threat, processes or technologies.

This report explores the key steps NHS organisations can take in improving their approach to security and maintaining the trust of the UK public and their staff.

Tim Hearn, Director, UK Government and Public Services, VMware

David Houlding, Director, Healthcare Privacy & Security, Intel

[1] http://www.wired.co.uk/article/nhs-trusts-affected-by-cyber-attack

[2] https://www.ncsc.gov.uk/news/latest-statement-international-ransomware-cyber-attack-0

[3] http://www.independent.co.uk/life-style/gadgets-and-tech/news/nhs-cyber-attack-medical-data-records-stolen-why-so-valuable-to-sell-financial-a7733171.html

[4] http://www.bbc.co.uk/news/health-40608253

About this research

VMware commissioned research to explore how cyber attacks on the NHS are impacting its ability to provide care and protect the sensitive and personal data that it holds. On VMware's behalf, independent research house Opinion Matters questioned 100 NHS IT decision makers and 2,000 members of the UK public about their view on the cyber threat to the NHS. The research was carried out between June and July 2017.

The challenges of protecting patient data

The NHS holds data for more than 65 million patients and employs 1.5 million people[5]. There is an enormous amount of complexity involved in ensuring that patient data is always accessible. This need for accurate, real time insight is only increasing given the growing use of data to help patient outcomes.

The NHS deals with over a million patients every 36 hours, creating a huge amount of data which needs to be accessed by an incredibly diverse array of devices. The IT infrastructure that sits behind every interaction with a patient, from diagnosis to treatment, is therefore more important than ever. The NHS recognises this and there have been a number of technology-based projects over the last few years that aim to make the best use of the data that we now have at our fingertips to inform and ultimately improve the care process. Some of the projects haven't had the success that they hoped for but for the ones that have succeeded, the benefits have been life-changing.

Unfortunately, it's the failed projects that make the headlines, and with little communicated about the thousands of IT-focused projects that take place within the NHS, it's unsurprising that the majority (70%) of the public respondents believed that too little is being invested in IT security.

As the increasing cyber threat is making almost daily headlines, promoting these successes is important.

To meet this increasing sophistication head on means involving everyone in the protection of the NHS – from the board and IT leaders to the clinicians and operational staff. That said, IT teams and NHS organisations are an invaluable part of ensuring that the IT environment is as safe as it can be. Unfortunately, the research revealed that expertise in IT security is lacking and risks further reduction. More than a quarter (28%) have lost skilled staff following a cyber-attack, while 38% believe they or their team lack the suitable skills to improve the NHS's cyber security infrastructure and strategy. This is worrying: without the right expertise, individual organisations within the healthcare system may be putting data at risk of being stolen or leaked, and of systems being shut down.

NHS IT teams acknowledge that threats to their organisations' security come from external sources such as hacktivist groups (50%) and individual cyber criminals (49%). However, they are also aware of an insider threat – labelling their own staff (32%) and patients themselves (30%) as significant risks. Although these insider leaks may not always be intentional or malicious, if patient data is accidentally accessed by someone it shouldn't be, the effects could be severe.

That suggests that there needs to be action on two different levels: from a technology standpoint, the NHS needs to invest in expertise and secure technologies, and from an awareness perspective, cyber security training is essential for all NHS employees – particularly when considering the number of data breaches made by NHS trusts over the last ten years. Public perception is also a concern. Two-thirds (66%) say they're concerned about the NHS' ability to protect their data from a successful attack and only 15% said they completely trust the NHS to protect their data. The NHS needs to act now to change that perception.

[5] http://www.nhs.uk/NHSEngland/thenhs/about/Pages/overview.aspx

A growing threat:

65%

of IT decision makers at NHS trusts believe threats are **growing in sophistication**

70%

say more needs to be spent on **IT security**

What's being targeted:

say hackers have definitely infiltrated **electronic patient data**

Electronic staff records are the

Consequences of successful breaches:

2 in 3

say attacks on equipment or facilities could result in harm to patients

59%

believe leaked healthcare data could have a harmful impact on patients and UK security

29%

have had to cancel or postpone appointments

1 in 4

have had to halt a research project

What does this mean for the UK and its citizens?

The IT decision makers surveyed are seeing attacks growing in frequency (44%) and sophistication (65%), posing a huge challenge for IT teams already struggling with limited funds, an explosion of data, and the increasing importance of technology in providing care to the UK public.

According to the ITDMs survey, sensitive and personal patient data has already been compromised and this is likely to happen again as the threat sophistication continues to evolve. Nearly a third say that electronic patient data has definitely been infiltrated and 78% that patient admin systems have or could have been infiltrated. Perhaps surprisingly, the most compromised data relates to NHS staff, with 80% saying that electronic staff records have or may have been infiltrated. This data – which includes bank details for payroll use – is a potential goldmine for hackers given the NHS is one of the world's biggest employers, with over 1.5 million[5] employees.

As well as threatening our most sensitive information, cyber attacks can have a significant impact on the NHS organisation's ability to provide care and carry out life-saving research. In fact, 29% of the survey respondents said that appointments have been cancelled or postponed following an attack. The recent WannaCry hack, for example, saw 48 trusts hit struggling to reschedule operations, with outpatient appointments cancelled amid the chaos caused.

Attacks can also have a devastating effect on the life-changing and saving research with which the NHS is involved. 26% of respondents said that they have had to halt a research project as a result of an attack. Research into new treatments and diagnoses is essential to improve health across an ever-growing population that is living longer.

If the NHS doesn't improve its approach to security, patients and staff could be at the very least highly inconvenienced and in the worst case, harmed. At a macro level, 59% believe that valuable healthcare data hacked or leaked could have a harmful impact on the UK's national security. Serving the majority of the UK's 65 million inhabitants - all of which the NHS holds sensitive and personal information on - makes it a potential weak link in protecting the UK from malicious outside threats.

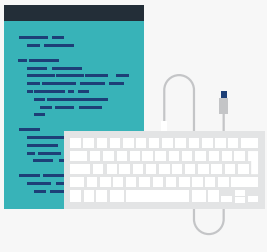
At a personal level, 62% say attacks on equipment or facilities could result in patients coming to harm. For example, an attack on an NHS network could halt trusts' ability to provide emergency care, putting those patient's lives at risk. It's not just the IT decision makers that are concerned - 72% of consumers surveyed believe a cyber attack would impact the level of care that they receive.

We put our lives in the hands of the NHS – it's important that we can do so confidently.

There's a skills gap:

OVER 1/4

(28%) of respondents said they lost skilled staff following an attack



OVER 1/3

(38%) lack the skills to improve cybersecurity

[5] http://www.nhs.uk/NHSEngland/thenhs/about/Pages/overview.aspx

What can be done?
Advice from the experts

"This is an exciting and challenging time for the NHS. New technologies, such as artificial intelligence and robots, promise to streamline and improve the care process, as well as research into treatments and cures. The life-changing impact of these technologies, however, is in danger of being overshadowed by heightened security concerns in light of an increasingly sophisticated and aggressive cyber security landscape. In fact, the introduction of more automated solutions reduces the opportunity for human error and should ultimately create a more secure NHS. More needs to be done to highlight the amazing work that is already being undertaken in NHS organisations across the country to introduce these new technologies and the positive impact that they are having on the care experience."

Tim Hearn, Director, UK Government and Public Services, VMware

---

"The NHS, like other public-sector organisations, faces the complex challenge of adopting innovative technologies whilst ensuring that the health sector is not vulnerable to an evolving cyber threat. The frequency of cyber attacks against the NHS has meant that public concern over the safety of patient data has only grown.

As recent events have shown, we cannot afford to delay implementing actions that can protect patient data. IT leaders across the NHS must have cyber security as a top tier agenda item in order for patients to receive the benefits of a digitised healthcare system."

Talal Rajab, Head of Programme, Cyber and National Security, techUK

What can be done?
Advice from the experts

"Patients are, rightly, worried about the NHS' ability to resist large scale cyber attacks, particularly following the WannaCry incident. The impact and disruption caused saw many organisations reverting to paper processes to continue to service the patients in their care. This is testament to the NHS's resilience, and the work that was put into planning for large scale incidents, such as WannaCry, was no different. As the threat increases, it will need to ensure that the systems and processes that underpin the care model are not liable to disruption. Cyber security investment needs to move beyond the traditional prevention and into limitation, investigation and recovery. Only then will patients' trust return."

Adam Louca, Chief Security Technologist, Softcat

"Many breaches and ransomware attacks including WannaCry are untargeted, opportunistic, and use propagation techniques such as computer worms exploiting unpatched systems, phishing emails, or other efficient broadcast methods. These attacks, as well as internal breaches, tend to affect organizations lagging in security and relatively vulnerable. The impact has been severe, including disruption of healthcare services across multiple NHS Trusts as well as other healthcare organizations worldwide, and has resulted in compromised patient safety and trust. The challenge has been: how can healthcare organizations determine if they are lagging and relatively vulnerable, and if so specifically in what safeguards? Benchmarking the security of healthcare organizations against the industry and peers can provide this pertinent information, and enables healthcare security teams to prioritize efforts, and rally support to allocate resources required to proactively remediate gaps to reduce risk."

David Houlding, Director, Healthcare Privacy & Security, Intel

"The UK Government must make public confidence in clinical and personal data a priority, otherwise it undermines efforts to expand care into the community using technology to achieve this cost effectively. There is a window of opportunity to grasp this and achieve world class status."

Tim Hearn, Director, UK Government and Public Services, VMware

What is the government doing?

Leadership, support and guidance at a government level will be crucial to driving forward a more secure NHS. The good news is that plans are already in place to introduce positive changes. The recent Government Response to the Data Guardian Review, the 'Your data: Better security, better choice, better care' report, demonstrates that the government is committed to enabling greater use of data in a safe, secure and legal way.

This response is an important step towards providing solutions to many of the issues and challenges that the NHS faces when it comes to introducing a safe and secure flow of information and data throughout the healthcare system. Key elements of the report include:

- Putting in place system security and standards that are appropriate to today's threat landscape, including the adoption of 10 data security standards and an updated Information Governance Toolkit
- Increased ownership at a local level with a new 'statement of requirements' clarifying required action, to be responded to with an annual 'statement of resilience' to ensure that standards are being implemented. Part of this will be for each organisation to name an executive Board member responsible for data and cyber security
- Boosting investment over and above the Spending Review's £50 million with an additional £21 million of capital funding to increase the cyber resiliency of major trauma sites in the first instance and moving forward, the NHS Digital's monitoring and response capabilities
- Answering the call from the UK public for greater transparency and control around how their data is used through a digital service, rolled out from December 2018, where the public can see who has accessed their summary care record. By March 2020, they will also be able to use online services to see how their personal data, collected by NHS Digital, has been used for anything other than direct care. Finally, people will be given the choice to opt out of sharing their data beyond direct care
- Organisations will face more severe penalties for data breaches and reckless or deliberate misuse of information once the NIS Directive is enforced in May 2018

Five steps for fighting cyber attacks

1

Secure board-level buy-in

To ensure that a strong, consistent security strategy is adopted throughout NHS organisations, it needs to be led from the top. As the security situation becomes increasingly concerning, cyber security needs to be put on the board level agenda, alongside other issues such as funding and staffing. Often, IT security is viewed as an insurance policy rather than a fundamental element of an organisation's IT and the 10% of IT spend that's put towards security if reflective of that. Creating a more secure NHS will require a cultural shift to focus on people, process and technology. If the Chief Executive, board and IT leaders are prioritising security, the internal culture will filter down so that everyone understands the severity of the threat and their role in mitigating risk. With the drive for increased ownership at a local level, as mandated by the 'Your data: Better security, better choice, better care' report, this guidance from the top will be more important than ever.

2

Share the responsibility

The security of the NHS is no longer the sole responsibility of its IT teams. As the NHS is increasingly digitised, the role of technology within healthcare is only going to grow, and so will the devices used in the care process. With human error one of the weakest links when it comes to the security of any organisation, NHS trusts need to educate every member of staff about the key role that they play in the fight against the threat of malicious attacks. Creating a security conscious culture, where everyone in the organisation is aware of the risk and understands the individual part they play, is vital.

3

Balance freedom and control

Cyber security is a balancing act, maintaining an acceptable security posture, whilst providing NHS staff with the freedom to carry out the task in hand and ultimately provide the public with world-class healthcare. There is a change in perception on IT teams, in that they are now being seen as enablers, providing clinicians with the tools to make their jobs easier and time more effective. This advance in technology can also increase the threat plane, and so IT teams need to maintain an appropriate level of control and visibility.

4

Stay up to date

The hackers who carried out the WannaCry attack in May 2017, which severely impacted a number of NHS organisations across the UK, exploited a vulnerability in the NHS' IT environment. In many cases, IT teams had pushed out the security patches but the machines were not re-booted, and therefore the patches were not effective. IT must work with the end-users of the technology and create a process for ensuring that these patches are being carried out. This is an area where automation can play a key role, formalising and automating the security process to help mitigate this risk.

5

Protect from the inside out

The traditional approach to security, which focuses on protecting the perimeter of an organisation's IT environment is outdated and no longer provides the level of protection that the NHS needs. This approach means that once a threat enters the network, it has free reign to move between applications, accessing whatever data it encounters. This is a particular issue within healthcare, as many of its legacy applications used to treat patients also have some form of known vulnerability making them soft targets. By introducing micro-segmentation, NHS IT teams can shrink-wrap security around each workload, putting in place firewall rules at the level of each application and Virtual Machine.

Conclusion

In our increasingly digital-led world, information and data is a fundamental part of the care process. The NHS needs to demonstrate to the UK public and its staff that it is doing everything it can to protect their personal and sensitive information. It needs to improve the trust of UK citizens, as this will enable the public to embrace the benefits that greater transparency and data sharing between NHS organisations, with third parties for research purposes, can bring. This data sharing is so important for the future of healthcare but NHS organisations can't do so without the approval of the UK public.

Budget cuts coupled with an increasingly aggressive cyber threat means introducing these changes is a daunting task. However, this is not a 'one-time fix', and should be approached as an ongoing transformational journey that will constantly evolve. Technology can provide the platform to future-proof this approach. The good news is that recent high-profile attacks have galvanised the government into action and investments and changes are already being made to create a more safe and secure NHS.

As one of our most beloved and respected institutions, the UK public want the NHS to succeed. The technology and skills are out there – it's now a case of working together the meet the cyber threat head on.

About VMware

VMware, a global leader in cloud infrastructure and business mobility, helps customers accelerate their digital transformation. VMware enables enterprises to master a software-defined approach to business and IT with its Cross-Cloud Architecture™ and solutions for the data center, mobility, and security. With 2015 revenue of $6.6 billion, VMware is headquartered in Palo Alto, CA and has over 500,000 customers and 75,000 partners worldwide.

About Intel

Intel (NASDAQ: INTC) expands the boundaries of technology to make the most amazing experiences possible. Information about Intel can be found at newsroom.intel.com and intel.com.

VMware & Intel on Security:

VMware and Intel transform security by providing comprehensive security measures based both in software and hardware across the data center and public and private clouds to enable secure application infrastructure, allowing for granular, micro-segmented security controls aligned to applications. Securing identity and endpoints protects a full range of devices and provides secure connections between applications on devices, data centers and clouds—unifying security, mobility, and networking with east-west traffic inspection and automated remediation against zero day threats. VMware's software layer over infrastructure and the Compliance Reference Architecture Framework streamline compliance by linking software, hardware, regulatory control, and independent audit validation.

VMware UK, Flow 1 & 2 River Park Avenue Staines-Upon-Thames TW18 3FA Tel: 01276 414300 www.vmware.com/uk