AbedGraham
Healthcare Strategies

The Healthcare Cyber Crisis:
How Technology Vendors Need to Respond

A White | Paper

Dr Akshay Garg
Dr Roshan Vara

Global healthcare continues to suffer from the year-on-year growth of cybercrime. In an industry that consumes and creates large quantities of sensitive data, the potential for a targeted cyberattack to cause mass patient harm is a real possibility. The fallout of the WannaCry ransomware attack has highlighted an urgent need for healthcare providers to consider cybersecurity solutions as a part of their digital roadmap. With a myriad of developing standards in data protection and security at local, national, and international levels, cybersecurity vendors have the difficult task of navigating a complex market landscape. This white paper explores the events that unfolded during the recent global attack and outlines how technology vendors should respond in order to engage with the needs of healthcare providers.

Cost of Failure

Healthcare is in the top three most frequently targeted industries in 2016, with estimated costs in the tens of billions of dollars annually.

Consultancy UK

Key Findings

'WannaCry' in the NHS

On May 12th at 06:02, the first reports of a healthcare cyberattack filtered through social media channels. Criminals had exploited the leaked EternalBlue/MS17-010 vulnerability built into all versions of Windows except Windows 10, using the self-replicating ransomware Wanna Decryptor (WannaCry). The ransomware spread across 150 countries, affecting over 300,000 computers, and major institutions including the UK's National Health Service (NHS).

Various reports suggest that as many as one in four trusts were infected, as well as multiple general practice surgeries and various allied healthcare services such as ambulance services and pharmacies. Patient harm has undoubtedly occurred due to diverted services, delayed appointments, missed treatments, and cancelled surgeries. **And at AbedGraham we firmly believe it was fortunate that the NHS was not specifically targeted by this attack**, although there is now a significant risk that healthcare providers will continue to face the possibility of focused attacks with the aim of causing direct and potentially lethal harm.

An FOI request by AbedGraham revealed that affected hospitals have reported their figures for cancelled outpatient appointments and inpatient procedures (e.g.

surgeries) to the Department of Health, but these are not, at present, publicly available. Even if these figures were available, it would be extremely difficult to estimate the financial cost to the trusts. Although there has been media speculation, it is AbedGraham's opinion that such predictions lack an appreciation of the complexities in clinical and financial operations. For example, in an acute care setting, it is difficult to quantify the loss of staff time and resources. In addition, cancelled outpatient appointments or inpatient procedures may lead to missed targets unless the trust is able to reschedule them in time and in such cases while penalties for missed targets may not apply, there would be an opportunity cost associated with the rescheduling.

Responsibility

"All health and social care organisations should provide evidence that they are taking action to improve cybersecurity."

Dame Fiona Caldicott
(June 2016)

The one area that can be quantified is the financial penalty associated with data breaches. In this cyberattack, the objective was not the theft of patient data, however such attacks are likely to increase too. Consequently, it cannot now be understated; **proactive healthcare organisations need to be cognizant of the looming EU GDPR, and the punitive measures that would be in place for failing to meet data protection regulations in addition to local penalties.**

European Fallout

WannaCry clearly highlighted the deficiencies in cybersecurity within the NHS, especially considering that no other EU country's health system suffered a breach at an institution-wide scale. Ireland and Slovakia suffered the effect of WannaCry in only one healthcare site each. Ireland took the approach of taking its entire system offline and the single affected site was outside this network. Norway and Denmark, two of the EU's most digitally mature healthcare providers had negligible effects on their IT infrastructure, with no major reports of healthcare organisations being affected.

Throughout Europe, major national and continental bodies are looking to evaluate their security standards and response to WannaCry. Importantly, the European Commission has highlighted the need for a co-ordinated response. With initiatives such as the Digital Single Market driving integrated models of care and the sharing of patient information across borders, EU member states will need to consider how they handle data outside the confines of their national hospitals. There is a risk that continued silo working will be an insufficient response for an EU-wide targeted attack. It is therefore imperative that a standard is set for cybersecurity across the bloc, perhaps leveraging the position of the EU Agency for Network and Information Security and Europol to steer a pathway for the protection of health data and ultimately patient care.

A Growing Trend

WannaCry is not the first incident of cybercrime affecting healthcare organisations; in 2016, several German hospitals were held to ransom over health data. At least 30 NHS trusts were the victim of ransomware attacks in 2016. And recently in Ireland, there were 5000 cyberattack attempts directed at one major Irish hospital over the course of a weekend. Responding to such attacks and to WannaCry, some hospitals take the drastic measure of taking all systems offline which in turn disrupts care delivery. This may represent a lack of trust with existing information systems management, IT infrastructure and business continuity plans, reflective of a centrally-driven approach, lacking organisation-specific detection and management measures.

Leadership

"Own the issue at senior leadership level…empower through training and learning personal responsibility in data security."

Dan Taylor
Head of Cybersecurity at NHS Digital

Cybersecurity in Healthcare

Healthcare Landscape

The healthcare IT industry is at different stages of maturity in the United States (US) and in the United Kingdom (UK). This is partly due to the privatised versus nationalised nature of the systems respectively, but perhaps more importantly it is due to the role of the government in advancing the digitisation efforts. While the US delivered 'Meaningful Use', the UK was left with the disastrous 'NPfIT' (National Programme for Information Technology). Consequently, over 85% of US physicians across primary and secondary care now routinely use an electronic health record (EHR) whereas the UK's NHS is playing catch up. The NHS can, however, boast close to 100% uptake in EHRs in primary care though secondary care EHR usage is far lower even considering the multiple procurements recently. Unfortunately, despite being able to learn from the challenges facing US healthcare providers, cybersecurity has not been a priority and not formed a core part of the procurement process for health IT solutions in the NHS. The havoc caused by an untargeted and technically basic ransomware, makes the prospect of an advanced targeted cyberattack particularly troubling.

Additionally, unlike many of their US counterparts, NHS trusts are effectively non-profit organisations, and it would therefore **be prudent for cybersecurity vendors to demonstrate more than just a financial incentive to deploy their specific solutions.**

Targeting Healthcare

Broadly speaking there have been two types of cyber incidents that have affected healthcare to date – denial of access and data theft. The motive behind these attacks is almost always financial, and for this reason targeting healthcare is a growing trend

in global cybercrime. Data theft is particularly problematic in the US where medical records are sold on the 'black market' at 50 times the value of credit card or social security numbers. Denial of access attacks are arguably worse due to the urgency and potential for harm they create, making it far more likely for a healthcare organisation to pay a ransom. This is of particular importance in areas such as critical care, where loss of access for even minutes could prove potentially fatal – **Dr Saif Abed, Founding Partner at AbedGraham wrote about this very subject almost a year ago in an article entitled "Ransomware will Kill a Patient".**

A Valuable Target

*"Electronic health records sell for **$50 per chart** on the black market, compared to $1 for a stolen social security number or credit card number."*

FBI Cyber Division

As health systems become increasingly interconnected with smart devices, mobile working, and interoperable systems, they naturally provide a larger threat surface area for cyber criminals. Cybersecurity solutions are important but *"security practices must be built in, not bolted on"* (Department of Health and Human Services, US). This requires vendors to understand some of the complexities that exist in healthcare – an industry that holds information more sensitive than financial services, and has a higher potential for harm than the energy sector. It also relies heavily on legacy systems, and many highly interconnected systems compared with other industries which have more closed systems. These factors make the healthcare industry simultaneously the most attractive and the easiest to target for cyber criminals.

People, Processes & Technology

Healthcare organisations are generally large entities with a whole range of people delivering, often patient-facing, services. The NHS in England, for example, employs over 1.1 million people, who can broadly be split evenly into clinical and non-clinical staff. The 'people' risk is therefore enormous and the entire service is reliant on the workforce having access to the correct information at the correct time. The balancing act between data security and patient care requires an understanding of the clinical workflows. Trusts recognise that technology is not enough, and a good example is the NHS Southport & Ormskirk Trust who published the following in their Board Meeting Agenda – *"Whilst technical controls were in place to prevent an attack, it was, however, recognised that these may be compromised due to lack of staff awareness, which constituted the biggest risk in light mainly of the increasing use of social engineering to elicit confidential information."*

Figure 1: AbedGraham's Six Steps of Cyber Awareness for Clinicians

Security Culture

"Protecting patients through good information security practices should be as second nature to the healthcare organization as sanitary practices."

US Department of Health and Human Services

Therefore, it is imperative to build a security culture, akin to that of hand hygiene in the clinical setting. AbedGraham has developed its own version of the 'hand hygiene' protocol that is prevalent across healthcare organisations (see Figure 1). Furthermore, because business continuity is so important, there must be processes in place in the event of a denial of access attack. Shutting down systems and preventing access to key data is not an effective solution in a healthcare environment. **Vendors with cybersecurity solutions that fail to address the 'people and processes' component are unlikely to succeed in evolving healthcare systems such as the NHS, regardless of how innovative their technology may be. AbedGraham fundamentally believes that vendors who can demonstrate their understanding of the complex workflows in the pre-sales process are much more likely to succeed in a growing market of demand.**

Our Recommendations

With the increasing number of cyber incidents occurring in healthcare, providers taking a reactive approach to protecting patient data is no longer an acceptable stance and consequently there is an evolving market demand for technology vendors to secure sensitive data. However, before approaching the healthcare market, vendors will require the requisite knowledge of:

- The threat surface area present in the healthcare ecosystem and how this will evolve with the roll out of local and national transformation programmes.
- The key policies underscoring the handling of sensitive data (e.g. the UK's Caldicott Review, EU GDPR etc.).
- The complexities of clinical information workflows.

It is AbedGraham's belief that for technology vendors looking to succeed in the European public-sector healthcare market they must understand the complex web of workflows, both clinical and technical, that are present within a healthcare organisation. This vertical-specific knowledge will allow them to better comprehend the issues that are facing providers, and to better tailor their message for the market.

About AbedGraham

AbedGraham is Europe's leading, exclusively clinically based, healthcare IT strategy, operations and risk consultancy. The organisation's combination of clinical and strategic expertise is utilised by global IT infrastructure industry leaders to shape corporate strategies, clinical engagement and leadership initiatives, business case developments, major project bids and project management processes to maximise the positive impact of their solutions for healthcare providers. For more information, visit http://www.abedgraham.com or follow on Twitter at @AbedGraham.

Contact the Authors

Dr Akshay Garg BSc MBBS, Clinical Strategist, AbedGraham
E-mail: agarg@abedgraham.com

Dr Roshan Vara BSc MBBS, Clinical Strategist, AbedGraham
E-mail: rvara@abedgraham.com