WHITE PAPER

Protecting Data in the Healthcare Industry

An Osterman Research White Paper

Published July 2017

Osterman Research, Inc.
P.O. Box 1058 • Black Diamond, Washington • 98010-1058 • USA
Tel: +1 206 683 5683 • info@ostermanresearch.com
www.ostermanresearch.com • @mosterman

EXECUTIVE SUMMARY

Criminals focused on getting a financial return from cybercrime have identified a particularly attractive target: the healthcare industry. The industry has a set of characteristics that make it ideal for all kinds of cyber attacks, including:

- Preventing access to IT systems immediately triggers life-and-death consequences for patients under care, ensuring that a resolution becomes of critical urgency for the healthcare provider. If a doctor or nurse cannot read a patient's electronic health record to review critical health information, for example, a patient could be given a life-threatening prescription or the wrong procedure, leading to significant legal liability.
- Stealing healthcare records is a lucrative business because of the inclusion of most of the personal, medical, and financial information a criminal requires for identity theft, medical fraud, financial misdemeanors, tax fraud, and insurance fraud, among others. In short, it's the ultimate cheat sheet, and given that most of the core identifiable information can't be changed (such as a person's date of birth and Social Security number), it offers value for years to come.
- Crippling IT systems is comparatively easier than in other leading industries because of systematic underinvestment in IT security within the healthcare industry, along with difficult-to-update medical devices that continue to run outdated and vulnerable operating systems.
- An out-of-date mindset that cyber security is all about safeguarding patient data – which is the focus of much of the regulation that defines the minimum standard – rather than the new reality that cyber security is about ensuring the ability of a healthcare institution to function.
- An industry-wide lack of trained cyber security professionals, since much of the recent focus within the healthcare industry has been on implementing electronic health records systems (EHRs) under externally-imposed tight deadlines. With many IT professionals in the sector focused on new and emergent EHRs, there are new vulnerabilities and weaknesses to exploit.
- Well-known cases in which healthcare providers have paid the ransom to reverse a ransomware infection because of a lack of backup capabilities, process failures, and the general urgency to get back to business as quickly as possible (since lives are at risk). Getting a reputation as a soft target is not a good thing.
- Interestingly, healthcare "is the only industry where employees are the predominant threat actors in breaches.[i]"

Healthcare "is the only industry where employees are the predom-inant threat actors in breaches.

KEY TAKEAWAYS

The healthcare industry finds itself under cyber attack from many vectors, including ransomware, malware and targeted attacks. While these attacks specifically cause direct harm to IT systems, it's the flow-on effects that have the industry reeling.

Cyber attacks are able to:

- Undermine the ability of a healthcare provider to function. In the WannaCry ransomware attack in mid-May 2017, for example, hospitals across the United Kingdom had to divert incoming patients onboard ambulances to other hospitals, cancel surgeries that were within minutes of starting, and revert to tedious manual processes for critical care situations. Even basic processes like admitting a patient and printing a wrist band were compromised. The survey conducted for this white paper found that one in ten organizations surveyed were impacted by WannaCry.
- Encrypt the electronic health records system at an institution, preventing access to core health data on patients currently under care. Healthcare professionals must return to paper-based processes for critical care situations, a work-style for which digitally native doctors and nurses may have never been trained.

©2017 Osterman Research, Inc.

- Exploit vulnerabilities in state-of-the-art medical devices that operate on outdated operating systems, such as CT scanners and MRI devices. This prevents their use for day-to-day diagnostic and analysis tasks, causing immediate consequences for patients under care, and costing enormous amounts in lost revenue per day.
- Prevent the use of standard everyday communication tools, such as phone systems and email, making it difficult for doctors, nurses, and all other healthcare professionals to deliver patient care.
- Exfiltrate valuable patient data for sale on the black market, triggering data breach notification requirements for healthcare providers, thus opening themselves up for regulatory fines, reputational damage, and class action suits.

The key infection vectors for the healthcare industry are:

- Email attachments that masquerade as standard business documents, but carry or point to a malicious payload that introduces malware or holds the user's computer and connected devices for ransom.
- Web links that are disguised to look like a trusted site but point to a false and malicious destination. Link-shortening services are particularly dangerous because it is so easy for a convenient short link to hide a malicious destination.
- Drive-by-downloads from malicious web sites that exploit known vulnerabilities in out-of-date applications and unpatched operating systems.
- Advertisements on web sites and within applications that have been compromised, and carry a malicious payload. Since the user is visiting a known and trusted web site, the likelihood of being deceived by the malicious ad is higher.
- Free downloads of normally expensive software that have been changed to include malicious components, or that merely masquerade as expensive software. The malicious payload can install a persistent threat that records keystrokes, exfiltrates data, or holds the computer for ransom.
- USB drives that have become accidentally or intentionally infected with malware or ransomware. Plugging in the drive to share files with a colleague also introduces a malware or ransomware threat.

The good news is that protecting healthcare data during the previous 12 months has become a “higher” or “significantly higher” priority for 47 percent of the organizations surveyed for this white paper.

ABOUT THIS WHITE PAPER

This white paper is sponsored by Zix. Information about the company is provided at the end of this paper.

THE REGULATORY LANDSCAPE FOR HEALTHCARE FIRMS

There is a generalized recognition in many legal jurisdictions around the world that healthcare data is an especially sensitive type of personally identifiable information and must be protected from misuse. While the specific provisions and requirements have national nuances, the intent is essentially the same. Organizations managing healthcare data are subject to the following compliance requirements and regulations:

HIPAA (1996)

For US healthcare institutions, the Health Insurance Portability and Accountability Act (HIPAA) mandates a set of federal requirements for protecting individually identifiable health information. These apply to both "covered entities" (those providing direct care) and "business associates" (of which there are many and varied types).

©2017 Osterman Research, Inc.

The HIPAA Privacy Rule mandates protections for health information that's held or transmitted in any form or media, for data that can be associated with an identifiable person, such as the physical and mental health of a patient (past, present, and future expectations), the history of healthcare given to a patient, and payment mechanisms (past, present, or future).

The HIPAA Security Rule requires that healthcare institutions put in place appropriate administrative, physical, and technical safeguards to assure the confidentiality, integrity, and availability of protected health information. For example, if data has to be sent to another person or institution and there is a significant risk of unauthorized disclosure, data encryption is required.

Finally in terms of HIPAA, there is a recognition that healthcare workers themselves need to be ever vigilant of privacy and security issues. Section 164.308(5) requires that every organization in the US healthcare industry offer a security awareness and training program for its staff, including management.

HITECH ACT (2009)

The Health Information Technology for Economic and Clinical Health Act (HITECH) was introduced in the US in mid-February 2009, as part of the American Recovery and Reinvestment Act (see details below). It offered billions of dollars in funding for building a national interoperable medical records system, introduced a data breach notification requirement (Section 13402), and demanded evidence of tiered "meaningful use" of the medical records system by certain dates. Breaches of unsecured protected health information affecting 500 or more individuals are listed in a publicly accessible database managed by the US Department of Health and Human Services Office for Civil Rights. Clearly, healthcare organizations need the ability to know when they have been breached, and are required to share this publicly. The threat of public shaming and reputational damage appears to not have been sufficient given the almost 2,000 data breaches listed by the US Health and Human Services data breach web site in June 2017.[ii]

ARRA (2009)

The American Recovery and Reinvestment Act (ARRA) was passed in mid-February 2009, offering the United States a $787 billion stimulus package, including an allocation of $19.2 billion for healthcare. A core initiative in healthcare was a new interoperable electronic health record (EHR) enabling the secure exchange of patient health information across all involved providers across the nation, as well as giving patients online access to their own EHR. Healthcare organizations needed to demonstrate meaningful use to qualify for subsidy payments. An interoperable EHR introduces significant data privacy and security concerns for all healthcare providers, such as keeping your own patient data safe, securing patient data sent from other providers, and ensuring HIPAA privacy and security compliance by cloud EHR providers.

An interoperable EHR introduces significant data privacy and security concerns for all healthcare providers.

ACA (2010)

The Affordable Care Act (ACA) was introduced in March 2010, ushering in an era of significant healthcare reform for the United States. Among other provisions, it mandated the sharing of certain types of patient information between healthcare providers and the government. For example, Code Sections 6055 and 6056 require the collection of social security numbers of spouses and dependents for reporting to the IRS. The implication is that healthcare providers are now holding additional classes of sensitive information not just for patients, but for family members as well, information which must both be protected and shareable with government agencies under specific circumstances.

HIPAA OMNIBUS RULE (2013)

The HIPAA Omnibus Rule of 2013 introduced changes to various privacy and security requirements in HIPAA in order to bring them into alignment with the HITECH Act. New provisions include elevating the duty of care for protecting personal health information among business associates and their subcontractors (in addition to covered entities), increasing the penalties for noncompliance to a maximum of US$1.5 million per violation, adding genetic information to the definition of personal health information, and expanding the coverage of types of electronic media, among others.

©2017 Osterman Research, Inc.

GUIDELINES FOR mHEALTH DESIGN AND DEVELOPMENT UNDER HIPAA (2016)

With the increasing proliferation and usage of mobile devices across all stratas of the global population, healthcare providers are developing healthcare related apps and devices. The US Health and Human Services department published specific guidelines in January 2016 covering these so-called "mHealth" applications and devices. Essentially, any app or device that works with personally identifiable health information must comply with HIPAA, and if a HIPAA covered entity is involved with an app or device, HIPAA almost certainly applies. Note that non-personally identifiable health information, such as steps taken and distance covered, are excluded from the HIPAA requirements.

NATIONAL HEALTH SERVICE (UNITED KINGDOM)

The UK Data Protection Act of 1998 sets the legislative framework for healthcare institutions across the United Kingdom in relation to data privacy and security. Requirements include data minimization (collection of only the data that is required for a specific purpose), data security, data relevancy, and data currency. Organizations should not keep data for longer than necessary, and must provide access to the data subject when requested to do so. Data controllers – the entities responsible for controlling the data – are responsible for ensuring appropriate access controls are maintained, and guarding the data so it is not transferred into another legal jurisdiction without equivalent data security requirements.

The National Health Service (NHS) also offers a set of security policies and guidelines for NHS organizations in the public sector, with regional variations across England, Scotland and Wales. Provisions include mandatory annual training on information governance, and the establishment of processes for removing access rights to data and systems when an employee is terminated. The NHS Care Record Guarantee promises confidentiality and security of patient information, and the NHS Confidentiality Code of Practice sets out mandates when sharing information with other organizations.

NURSING & MIDWIFERY COUNCIL (UNITED KINGDOM)

The Nursing & Midwifery Council (NMC) is the regulator for nurses and midwives in England, Wales, Scotland and Northern Ireland. The NMC's Code sets out the professional standards expected of registered nurses and midwives, including privacy, security, and confidentiality of patient health information. Code 5 establishes people's right to privacy and confidentiality whether alive or dead, and sets out the determinants when deciding whether to share confidential patient data with others. Code 10 requires the maintenance of clear and accurate records, and the security of those records.

By virtue of their chosen occupation and the region in which they practice, nurses and midwives are also subject to the data protection guidelines in the UK's Data Protection Act.

BRITISH MEDICAL ASSOCIATION (UNITED KINGDOM)

As with the NHS and NMC, members of the British Medical Association (BMA) are subject to the UK's Data Protection Act. This covers the lawful use of personal and health data, the responsibilities of GPs (general practitioners) as data controllers, and the need for explicit consent from patients when sharing personal health information with other healthcare professionals and entities. Balancing the competing requirements around patient data privacy – in light of the Data Protection Act – is an issue of ongoing concern for the BMA.

The BMA has a couple of other resources related to data security, as well. The fourth part of its Confidentiality and Health Records Tool Kit, for example, outlines requirements for securing patient health information from both external and internal threats. It also expects members to follow professional standards, act in accordance with privacy conditions in an employment contract, and follow various other legislative and health industry requirements, such as the Access to Health Records Act of 1990, the Computer Misuse Act of 1990 (such as not accessing computer material under another person's user credentials), and the NHS Care Record Guarantee (for NHS England).

GENERAL DATA PROTECTION REGULATION (EUROPEAN UNION)

The new General Data Protection Regulation (GDPR) in Europe, due to be enforced from late May 2018, sets out the requirements for protecting personally identifiable information, with

©2017 Osterman Research, Inc.

special considerations required for sensitive information on natural citizens of the European Union. The GDPR harmonizes the data privacy and protection regulation of the 28 member states of the European Union, and requires the use of technical and organizational safeguards over covered information. There are significant financial penalties for organizations that fail to adequately safeguard personal data, breach notification requirements, and specific mandates around consent, the responsibilities of data controllers and processors, and the need for data protection assessments.

MEDICAL BOARD OF AUSTRALIA

The Medical Board of Australia works within the legislative framework established by the Australian Privacy Act of 1988 (and subsequent updates), which holds that health information is one of the most sensitive types of personal information that can be held about an individual, and thus must be subject to adequate protections. One recent update to the Privacy Act introduced mandatory data breach notifications.

The Medical Board separately has a Code of Conduct of Good Medical Practice, sections in which cover confidentiality and privacy of patient health information (Section 3.4) and control the security and access to medical records (Section 8.4).

AUSTRALIAN MEDICAL ASSOCIATION

As with the Medical Board of Australia, healthcare professionals are required to practice within the provisions of the Australian Privacy Act. The Association also has a Code of Ethics that addresses the protection of patient information (Section 2.2), with patient rights such as access, confidentiality, consent for disclosure, and that records will be kept securely. The Code of Ethics was introduced in 2004, and underwent substantial updates during 2016.

SUMMARY

Considering these many compliance requirements, it is impossible to get away from the fact that healthcare organizations have an elevated and broad duty of care for the health information stored on patients.

Healthcare organizations have an elevated and broad duty of care for the health information stored on patients.

TRENDS FOR HEALTHCARE PROFESSIONALS THAT HAVE INCREASED THE THREATS

An analysis of the healthcare industry highlights a significant number of trends that are converging to increase data privacy and security threats. Let's review those trends briefly.

HEALTHCARE PROFESSIONALS ARE INCREASINGLY USING CLOUD SOLUTIONS

As with the rest of the world, healthcare organizations are shifting various workloads to cloud services. As a consequence, healthcare professionals are using cloud-based file-storage and sharing services, cloud-based electronic health records services, and various cloud-based services for exchanging healthcare information between providers and other players in the industry. MarketsAndMarkets forecasted a tripling of cloud expenditure within the healthcare industry from 2015 to 2020,[iii] while HIMSS Analytics have tracked significant uptake for many types of cloud services by healthcare,[iv] with health information exchange and back office solutions the leading current workload in the most recent survey. The use of cloud services introduces a shared responsibility security model, the demand for new ways of securing sensitive information, and many new potential points of failure in security processes.

PHISHING AND RANSOMWARE ARE BECOMING MORE PREVALENT

The impacts of phishing and ransomware cyber attacks are getting worse across the world, and are having significant negative impacts specifically in the healthcare industry – Verizon has found that the healthcare industry is the second biggest target for ransomware[v]. SonicWALL reported that ransomware attacks grew from 3.8 million in 2015 to 638 million in 2016, a growth of 167 times in one year.[vi] Symantec tracked 4,000 ransomware attacks per day in the first quarter of 2016, a 300 percent increase year-on-year.[vii] Malwarebytes noted the increased use of ransomware in various malicious forms, with the share of malicious payload growing from 20 percent at the beginning of 2016 to 67 percent by November.[viii] It has also been

©2017 Osterman Research, Inc.

estimated that there are up to 1,000 new variants of ransomware being released to market, creating an incredibly challenging environment for organizations of all kinds. When ransomware affects healthcare organizations, lives are at immediate risk.

In terms of the healthcare industry specifically, consider the following:

- Verizon found that 72 percent of malware incidents in the healthcare industry are actually ransomware incidents[ix].
- IBM X-Force Cyber Security found that healthcare was the most attacked industry during all of 2016.[x]
- Cyber security Ventures said attacks in the industry were up 35 percent from 2015 to 2016.[xi]
- NTT Security reported that 88 percent of all ransomware attacks from April to June 2016 were focused on healthcare organizations.[xii]
- NTT Security reported in May 2017 that healthcare was the third most likely industry to be targeted by ransomware, with business and professional services in first place and government and government agencies in second.[xiii]
- The WannaCry ransomware attack in May 2017 was a broad-based attack across the world that infected more than 200,000 computers in more than 100 countries, but had headline-grabbing implications for hospitals across the United Kingdom, with 61 NHS organizations affected. Affected healthcare organizations had to divert inbound ambulances to other facilities, cancel surgeries, and re-schedule diagnostic tests and routine operations. A leading cancer hospital in Indonesia was also affected by WannaCry, causing healthcare professionals to revert to manual forms and workflows.
- There have been some suggestions that ransomware is becoming more insidious too, with the ability to increase the ransom payment depending on the type of information stored on the infected device. For example, the ransom can increase significantly if medical records software is identified prior to the encryption process beginning.

Finally, with reports that ransomware is now available "as a service," with proceeds from the criminal undertaking being shared with the ransomware developer, it is no surprise that the threat is greatly elevated. And, as various healthcare organizations have discovered to their detriment, it takes only one employee to mistakenly download a malicious document.

As an example of ransomware-as-a-service, a hospital that serves patients in southwest Washington and Oregon fell victim to a spearphishing email that included a shortened URL. Clicking on the link redirects the user to a cloud-based storage site that allows them to download a well-crafted and realistic-looking malicious .docx file. Clicking on any of three icons in the document triggers a JavaScript that executes a variant of the Philadelphia ransomware, available for just a few hundred dollars.[xiv] It takes only a single employee to mistakenly download the document and potentially infect an entire healthcare system.

Phishing, spearphishing, and CEO Fraud – all variants on the theme of delivering a malicious payload via email – are becoming more common and damaging.

- A basic phishing attack casts a wide net hoping to ensnare as many people as possible using forged emails and malicious attachments that most people expect to receive, such as shipping notifications, password change notifications, account notifications (such as PayPal or Amazon), and friend requests.
- Spearphishing is a more targeted attack on a specific group of people, with attached malicious documents or embedded malicious links that are carefully crafted to look valid to the recipient; the GoldenEye spearphishing campaign, for example, targets German speaking people in HR departments with a malicious Excel spreadsheet. With the many social networking services available today, such as LinkedIn and Facebook, a cybercriminal can piece together connections between people, and craft a very believable message with a valid sounding document attached to catch the unwary or distracted.

Phishing, spear-phishing, and CEO Fraud – all variants on the theme of delivering a malicious payload via email – are becoming more common and damaging.

©2017 Osterman Research, Inc.

- CEO Fraud (also commonly called whaling or Business Email Compromise [BEC]), is a phishing variant that goes after the "big fish," or those with the access rights to confidential data or financial authorizations to transfer funds. A common approach is a forged email from the CEO to the CFO, requesting a confidential transfer of funds to a specified bank account, in light of a new venture, acquisition, or other initiative. The email will often be specifically crafted to replicate the writing style and tone of the CEO, along with a demand for absolute secrecy.

DATA BREACHES ARE BECOMING TOO COMMON

Despite all of the regulatory requirements around data privacy, security, and preventing data breaches of personally identifiable health information, they have become all too common across the industry. For example, the survey conducted for this white paper found that 17 percent of the organizations surveyed have suffered a breach of healthcare-related data during the previous 12 months.

The 2015 data breach at Anthem saw the theft of medical records for more than 80 million people,[xv] while the breach at Premera, from 2014-2015, resulted in medical records for some 11 million customers being stolen.[xvi] One analysis of the US Health and Human Services data breach database found an increase from 268 data breaches in 2015 to 328 separate breaches in 2016, with more than 16 million health records of American citizens being affected.[xvii]

HEALTHCARE DEALS WITH LIFE-AND-DEATH SITUATIONS, AND CAN'T AFFORD THE DISRUPTIONS

Ransomware, phishing, and data breaches all compromise core healthcare systems, which immediately undermines the ability of the healthcare organization to deliver standard and emergency care to patients. It can be a matter of life-and-death when doctors can't access a patient's healthcare record, a hospital has to turn away patients onboard an ambulance, nurses have to revert to manual processes they haven't been trained to use, the pharmacy can't get timely alerts for new prescriptions, and medical devices are locked and inoperable. These are all life-critical situations, and patients, their families, and regulators expect near-perfect uptime and availability.

DISRUPTIONS UNDERMINE THE REPUTATION AND VALUE OF THE AFFECTED ORGANIZATION

For hospitals that have been compromised by ransomware, there are ongoing reputational damage and brand risks. For example, the Hollywood Presbyterian Medical Center was infected with ransomware in early 2016, and ultimately paid nearly $17,000 in Bitcoin to regain access to its own systems. The hospital was effectively out of action for 10 days, costing lost revenue. The longer term reputational impacts linger, however; for example, a Google search for the hospital puts the ransomware episode as four of the first 10 search results, leading potential patients and others to contemplate whether its health care performance is better than its competence in IT. Likewise, regardless of the great work done at the California-based health system, the impact of its recent $2.14 million fine for HIPAA security and privacy violations and the $28 million settlement of a class action suit will stay around for a long time.

With mandatory data breach notification requirements in an increasing number of jurisdictions, healthcare organizations have no choice but to tell the world when their security systems are inadequate. Data breaches and ransomware infections affect the value of the brand, and can have negative goodwill implications in a merger or acquisition situation. While not a healthcare example, consider the $350 million discount Verizon received on purchasing Yahoo! after the disclosure of two massive data breaches at Yahoo! over many years.[xviii] Perhaps it is no surprise that, according to Bitdefender last year, a majority of US organizations would rather pay a hidden penalty fee than have the details of a data breach go public.[xix]

THE HEALTHCARE INDUSTRY HAS SYSTEMATICALLY UNDER-INVESTED IN SECURITY

Security controls across the healthcare industry have received insufficient funding over many years. In England, for example, the government has appropriated capital funding set aside for

©2017 Osterman Research, Inc.

buildings and new equipment to pay for day-to-day services, such as Accident & Emergency departments.[xx] This has made it more difficult for NHS organizations to deploy the necessary preventative measures. In the United States, HIMSS Analytics and Symantec report that 80 percent of healthcare providers spend less than six percent of their overall IT budget on security, and 50 percent spend less than three percent.[xxi] This is in comparison to 16 percent for the US Federal Government. Other research studies have highlighted that security is an afterthought for many healthcare organizations, with some hospitals failing to deploy even basic security measures such as intrusion detection, security assessments of current infrastructure, and the ability to remotely wipe lost or stolen devices. The US Health and Human Services department called out the general lack of encryption across the industry, stating that some 60 percent of healthcare data breaches since 2009 could have been avoided if the data had been properly encrypted.[xxii] It's a sad state of affairs.

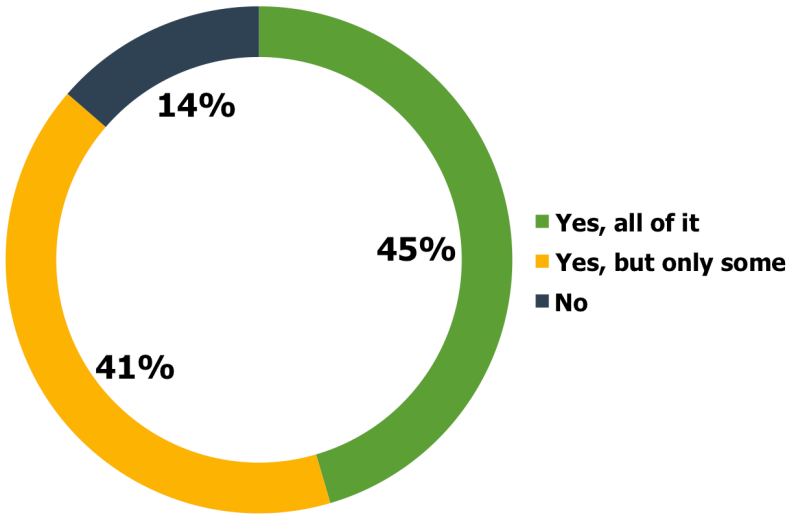
The survey conducted for this white paper found that most organizations either do not use encryption/tokenization of healthcare-related data at-rest, or they do not do so for all of their systems and applications.

WORKERS FACE A GROWING ARRAY OF COMMUNICATION AND COLLABORATION TOOLS

The final trend of note is the growing number and complexity of communication and collaboration tools being used across the sector. As with other industries, workers face an onslaught of interaction requests and demands through email, social media, new enterprise collaboration systems, texts, and mobile device apps. Workers on the front line of delivering healthcare trust that these systems are secure and reliable, but that is untrue and these tools are often used for malicious purposes masquerading as valid ones.

Security controls across the healthcare industry have received insufficient funding over many years.

Figure 1
"Does your organization use encryption/tokenization of healthcare-related data at-rest in systems and applications?"



Source: Osterman Research, Inc.

KEY CYBER SECURITY RISKS FOR HEALTHCARE PROFESSIONALS

The environment in which healthcare professionals work is fraught with cyber security risks. This creates a very challenging workplace to protect. Let's look at the risks.

- **Large attack surface**
  Medical care is no longer the domain of the generalist, but rather a complex collaboration between multiple medical specialists working for different organizations and interacting using disparate IT systems. Healthcare organizations have multiple geographical locations once different hospitals and outpatient clinics are accounted for. A modern hospital can have thousands of workstations, specialist medical devices running embedded operating systems, specialist medical software, mobile devices, and both on-premises and cloud-based services. Shared workstations are used by an ever-changing roster of healthcare professionals, and the urgency of the work means that generic user credentials are often used rather than individual user accounts. This means that systems are left wide open. With the push to interoperable electronic health records, sensitive patient data is continually flowing in-and-out of healthcare systems. These factors add up to an increased risk of being compromised, hacked, or breached.

- **Phishing and Spearphishing**
  Phishing and spearphishing are very common ways of distributing malicious email attachments and Web links. The banality of the subject matter for phishing, and the assumed-validity of spearphishing can make it difficult for time-pressed and stressed workers to identify when something isn't quite right. When the infection is an advanced persistent threat that lingers undetected for many weeks or months, the damage from these threats is significant.

- **CEO Fraud, BEC, Whaling**
  Carefully crafted emails that target the C-suite with spoofed addresses and calls for confidentiality can lead to a CFO transferring money to a criminal's account without being aware of the misdeed until it's too late. If the infection is a persistent threat on the other hand, given the generally wide access rights to data and systems held by senior executives, the threat of data breaches of health information, loss of corporate secrets, and being held up for extortion is high.

- **Ransomware**
  Ransomware is a significant threat to the data and systems of all organizations, but especially threatening to healthcare organizations due to the life-and-death consequences of not being able to run a hospital or other facility. With modern forms of ransomware able to not only infect the first machine but also automatically sniff out other vulnerable targets across the network, healthcare professionals can't afford to be the one person who gets it wrong. While medical records are among the most valuable data for sale on the black market, ransomware gets criminals an immediate payoff without having to sell anything.

- **Identity theft**
  Healthcare records contain all of the data points on an individual that are needed for identity theft, in addition to financial, tax, insurance and medical fraud. The healthcare industry has an abysmal track record in protecting patient data, with tens of millions of healthcare records breached in 2016 alone.

- **Malware and viruses**
  While ransomware currently gets all the attention as the weapon of choice by cybercriminals against healthcare, other forms of malware and viruses are just as pernicious. The widespread use of older operating systems that are unpatched due to their use within medical devices, vulnerable software plug-ins that have not been updated in a while, and medical devices that have not been security tested let alone hardened, provide an attractive target for infection. Even if the threat is not immediately triggered, a malware infection that lies dormant pending a future date or event should be ringing warning bells across the industry.

- **Data breaches and loss of patient data**
  Not everyone working for your organization is an honest and upright healthcare professional, dedicated to patient health and furthering the impact of the organization: some are hiding nefarious intent. These malicious insiders know where the juicy data is being stored, and may have elevated access privileges to the same systems leading to data breaches and loss of patient data. But it isn't just malicious insiders that are

©2017 Osterman Research, Inc.

dangerous, however; it is more often simple carelessness of well-intentioned workers who leave laptops logged in but physically unguarded, fail to lock a file cabinet when no-one is around, email a spreadsheet with PHI to the wrong party, or leave paper-based records spread out for others to see and steal. Endemic attributes of the industry are also to blame, such as failing to use encryption, not using unique usernames and passwords, failing to enforce logout, and not limiting concurrent user sessions.

- **Insider threats and the need for employee vigilance**
  With healthcare professionals covering a diverse range of specialist fields and having specialist IT system requirements, it can be difficult to identify the bad actor in the mix. When someone saves healthcare records to a different location on the network, for example, is that for a valid healthcare reason or because the person is in collusion with criminal outsiders for data exfiltration? When professionals don't follow healthcare industry requirements around user credential security, is that just a convenient way of getting work done faster, or carelessness that leads to unauthorized access of sensitive information and the next great data breach on the front page of the newspaper?

- **Users are a weak link in the security infrastructure**
  Healthcare workers have hectic schedules, work in life-and-death situations, and face significant change in systems and industry regulations. They are also, as with most other industries, the leading cause of all security breaches at the workplace. Current approaches to security training are not adequate—it is not frequent enough, it is divorced from day-to-day practice, and it doesn't register as being a sufficiently important part of healthcare practice. Healthcare professionals don't believe a ransomware infection or data breach will happen on their watch, and too often believe the best of others rather than being sufficiently skeptical to smell the proverbial rat. Healthcare organizations tolerate lax security standards, such as not enforcing strong passwords and automatic logout, and the general lack of investment in security over many years does nothing to create an environment where user-focused security is important.

- **Difficulties in managing healthcare systems**
  While every large organization faces challenges with keeping IT systems up-to-date, there are several factors at play in healthcare organizations that make it an especially difficult task. Medical devices, for example, are expensive to purchase, require re-certification after being updated, and are likely to break when updates and patches are applied. Likewise, specialist systems can be rendered inoperable when patches are installed, leading to a lower desire to fiddle with something that's actually working. Equally, the industry push to EHRs has consumed much of the discretionary IT staff resources and IT budget, leaving fewer staff available to develop the required expertise for cyber security. Despite these mega-risks, various research efforts have shown that even the basic things aren't being done, such as failing to remove inactive user accounts, not using encryption, and leaving default passwords active on databases that hold sensitive patient data.

- **Cyber criminals are focused on stealing healthcare records**
  Healthcare records are a particularly attractive target for cybercriminals, since they hold almost all of the information required for identity theft, social engineering, financial fraud, tax fraud, insurance fraud, and medical fraud. IBM's X-Force Cyber Security research stated that some 100 million patient records globally were breached in 2015,[xxiii] and the number of reported data breaches within the sector continues to rise. Research by the Ponemon Institute pegs the value of healthcare records at US$402 per leaked record,[xxiv] which is more than 10x the price of other breached data records on the black market. In the same vein, Dell Secure Works says that health records are 10-20x more valuable than credit card data;[xxv] while credit cards can be easily changed when fraud and unusual transactions are identified, the immutability of many of the sensitive data attributes in a healthcare record offer no such recourse. That is, you can't change your birth date or birth city, two data attributes that are used for all sorts of transactions.

- **Third parties can be compromised**
  Despite the best efforts of any one healthcare organization, the entire industry is at risk. With EHRs connecting organizations and the government across the entire healthcare delivery chain, if third parties have not sufficiently protected their systems, data you are responsible for may be compromised regardless of the precautions you have taken

Healthcare records are a particularly attractive target for cyber-criminals.

directly. While HIPAA and subsequent updates puts the burden of responsibility on the covered entity to ensure business associates and their subcontractors have adequate protections in place, it's an even more complex environment when multiple covered entities and various government agencies have intertwined data sharing mandates.

- **Staffing models can create security and data management problems**
  Volunteers and rotating staff members can create security and data management problems in healthcare organizations. For example, the "helpful person" from the community who is not adequately trained on IT security but uses a hospital computer during their lunch break to check their web-based email may inadvertently be the source of a ransomware infection.

- **Mergers and acquisitions create security risks**
  Healthcare organizations are not static entities, with mergers and acquisitions offering the promise of growth and financial reward. Bringing together healthcare providers with disparate environments causes security issues, including new cross-system vulnerabilities, outdated medical devices, and different models of access control. Organizations may find themselves managing multiple Active Directory forests and email services, which over time becomes complicated as the two organizations merge daily operations and cross-organization access control rights are necessary. While consolidation is critical to IT efficiency, application availability, data security and regulatory compliance, these initiatives are often delayed due to lack of budget and resourcing.

BEST PRACTICES FOR CYBER SECURITY DEFENSES

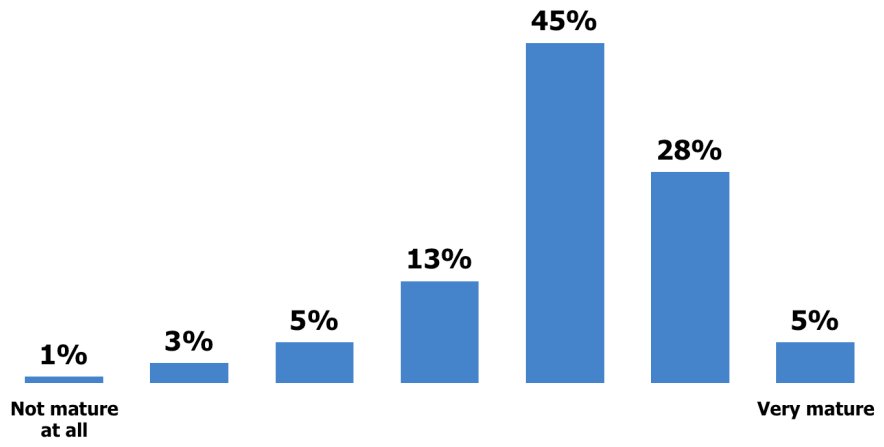
We have examined the regulatory landscape for healthcare firms, and both the trends and risks that drive cyber security threats in the industry. What should healthcare organizations be doing to strengthen cyber security defenses, particularly in light of the fact that healthcare is the only industry in which employees are the primary threat vector for data breaches[xxvi]? Here are the best practices.

- **Take the risks seriously**
  There is sufficient evidence across the healthcare industry that cyber threats including ransomware are a present and growing problem. Healthcare decision makers will need support from the C-suite and board of directors to elevate the importance of erecting appropriate defenses, and securing the appropriate budget and headcount. The vast majority of health IT decision-makers say security is rarely talked about at board meetings, which in light of its potential devastating effects, is a reality that needs to change. Senior executives play a vital role in setting the tone and culture of security mindedness within a firm; enhanced cyber security cannot be just an IT-initiative led by the IT team.

- **Build cyber threat awareness**
  Your organization faces generalized and specific cyber threats: generalized threats include ransomware, malware, and data breaches, and specific intensities of those threats due to the nature of the healthcare industry and its systems.

©2017 Osterman Research, Inc.

Figure 2
Perceived Maturity of Organizational and Technical Approaches to Healthcare-Related Data Protection Today



Source: Osterman Research, Inc.

- **Develop a cyber security strategy for your organization**
  Do the internal research to identify the specific threats faced at your organization, including a complete audit of current security tools, training programs, and security practices. This needs to be a comprehensive and enterprise-wide assessment, not a piecemeal approach. Elements include identifying specific risks, such as computers still running Windows XP, medical devices with unpatched operating systems, and printers in locations that non-authorized people could access. Assess the effectiveness of training programs, pulling data on metrics such as key offenders, repeat offenders, and the types of attacks that are consistently being successful despite training efforts. If outdated or vulnerable medical devices are of particular concern, work with the original vendor to develop solutions to the problem. When evaluating current and potential IT security vendors, look for those who are innovating at the rate of current threats, not those stuck in neutral. If your organization lacks the cyber security skills in-house to execute such a strategy, engage a specialist external consultancy to lead the effort.

- **Establish thorough and detailed policies**
  Translate your cyber security strategy into an appropriate number of thorough and detailed policies. These should include the communication and collaboration systems which are appropriately protected and secured for use (and those which are not), security tools that must be used (for perimeter, endpoint, and data protection), security practices that must be followed (such as keeping systems up-to-date), and acceptable and unacceptable use of corporate resources and personal devices connecting to the healthcare network. If healthcare professionals are permitted to use their own devices for enterprise purposes, what protections are necessary to ensure security of patient data, mitigate against lost or stolen devices, and protect the network from compromised devices or apps?

- **Enable encryption at every point**
  Encryption should be enabled for all sensitive or confidential data that is in-transit, in-use and at rest. Moreover, software and storage purchases should be made only if they support robust encryption capabilities. Where legacy applications and storage are not going to be replaced in the near future, third party encryption solutions should be implemented to manage this critical function.

- **Use threat intelligence to stay secure**
  With new threats constantly being released to market, use threat intelligence to highlight unexpected application, data and user behaviors, and move rapidly to isolate and contain questionable activities. Seeding your network with fake patient data can give early

Encryption should be enabled for all sensitive or confidential data that is in-transit, in-use and at rest.

warning of the presence of malicious users or advanced persistent threats, and user behavior modeling more generally can trigger alerts of employees starting to exhibit rogue behavior.

- **Test your ability to recover from a cyber attack**
  If your stated organizational policy is to never pay a ransom when infected with ransomware, you must fully test on an ongoing basis your ability to isolate an attack and recover from its effects. Invest in preparedness, such as multiple rotating backups, business continuity plans, and keeping systems patched to minimize the attack surface. But these must be tested, because finding out after an attack that a key element was missing is not good.

- **Invest in cyber security awareness training**
  Written policies and clear approaches for avoiding cyber attacks are necessary, but these have to become part of everyday healthcare practice. Security awareness training offers a structured approach for educating the workforce on current threats, red flags to look for in an email message or web link, how to avoid infection, and what to do in the case of an active exploit. Such training must be offered to all users and senior executives, since all are at risk. When training senior executives, ensure there is a section on identifying and responding to CEO Fraud, because this is key threat given their visible position within the organization. All users and executives will need repeated training episodes to stay current with the threat landscape, and new hires will require training during onboarding too. Since both HIPAA and the security policies of NHS England require ongoing security awareness training, it's clearly a best practice whose value has been widely recognized.

  The survey conducted for this white paper found that 44 percent of the organizations surveyed train employees on security awareness no more than once per year.

- **Govern user behavior for tools, devices, and repositories**
  Healthcare professionals should be following best practice guidance when using corporate-issued tools, devices, and data repositories, and especially so when using personally managed devices for accessing the same. Best practices include enforcing security updates before giving access, having the ability to remotely wipe lost or stolen devices, and limiting access to personal and sensitive data in corporate repositories. Connecting to public Wi-Fi networks is another common vector for attack, so either ensure appropriate protections are in place to mitigate the threat, or provide alternative ways of getting network access when out-and-about.

- **Tighten password policies and account access**
  With users often being the weak link in the chain, tighten password policies and account access to minimize the threat surface. Best practices include limiting access to only essential data resources, rather than giving people wide access to as much data as possible. Other best practices include active auditing of file access (to identify patterns of wrongdoing or questionable behavior), the ability to quickly revoke access to all healthcare systems when terminating an employee, single sign-on across all applications (for uniquely identifying access behaviors), and special controls for privileged accounts (such as top-level IT accounts required for system administration).

- **Have the right cyber security defenses**
  Strategies, policies, training, and preparedness are essential aspects of building cyber security defenses, but these human structures rely on having the right cyber security technologies in place. Healthcare organizations need advanced tools for blocking and identifying phishing attempts, blocking malware from entering the network via email and drive-by-downloads, and anti-ransomware capabilities for identifying abnormal application behaviors before they can take root on a device or across the network. Backups of core data are essential, application whitelisting is a good idea (although it is a big project), next-generation firewalls provide much deeper analysis and remediation of active threats, and endpoint security technologies keep a whole manner of devices safe from exploit. Last, but certainly not least, is the necessity of robust perimeter defenses that will block many of the threats that virtually all healthcare organizations encounter on a daily basis.

©2017 Osterman Research, Inc.

SUMMARY

The healthcare industry is among the most attractive targets for cybercriminals because of the high value of the information it manages; victimized organizations, such as hospitals, are often willing to pay ransomware demands; healthcare systems are normally easier to penetrate and disable because of a general level of underinvestment in cyber security; and there is a lack of security expertise in the healthcare industry. However, there are a number of steps that healthcare organizations can take – focused on implementing appropriate strategies, policies, processes, training and cyber security defenses – that will mitigate much of the risk that healthcare organizations face, making it a less attractive target for cyber criminals.

SPONSOR OF THIS PAPER

Zix is a leader in email security. Trusted by the nation's most influential institutions in healthcare, finance and government, Zix delivers a superior experience and easy-to-use solutions for email encryption and data loss prevention, advanced threat protection, archiving and bring your own device (BYOD) mobile security. Focusing on the protection of business communication, Zix enables its customers to better secure data and meet compliance needs. Its healthcare customers include more than 1,200 U.S. hospitals, 30 percent of Blue Cross Blue Shield organizations and many other covered entities and business associates. To learn about Zix solutions and set up a trial or demo, visit zixcorp.com.

www.zixcorp.com

@ZixCorp

+1 866 257 4949

©2017 Osterman Research, Inc.

© 2017 Osterman Research, Inc. All rights reserved.

No part of this document may be reproduced in any form by any means, nor may it be distributed without the permission of Osterman Research, Inc., nor may it be resold or distributed by any entity other than Osterman Research, Inc., without prior written authorization of Osterman Research, Inc.

Osterman Research, Inc. does not provide legal advice. Nothing in this document constitutes legal advice, nor shall this document or any software product or other offering referenced herein serve as a substitute for the reader's compliance with any laws (including but not limited to any act, statute, regulation, rule, directive, administrative order, executive order, etc. (collectively, "Laws")) referenced in this document. If necessary, the reader should consult with competent legal counsel regarding any Laws referenced herein. Osterman Research, Inc. makes no representation or warranty regarding the completeness or accuracy of the information contained in this document.

THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. ALL EXPRESS OR IMPLIED REPRESENTATIONS, CONDITIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE DETERMINED TO BE ILLEGAL.

REFERENCES

[i] Source: *2017 Data Breach Investigations Report*, Verizon
[ii] https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf
[iii] https://www.cloudcomputing-news.net/news/2016/jun/27/why-healthcare-industrys-move-cloud-computing-accelerating/
[iv] http://www.himssanalytics.org/news/health-it-and-cloud-5-must-watch-trends-2017
[v] Source: 2017 Data Breach Investigations Report, Verizon
[vi] http://www.csoonline.com/article/3176565/data-breach/ransomware-picks-off-broader-targets-with-greater-severity.html
[vii] https://www.barkly.com/hospital-ransomware-healthcare
[viii] http://www.zdnet.com/article/ransomware-is-about-to-get-a-lot-worse-by-holding-your-operating-system-hostage/
[ix] Source: 2017 Data Breach Investigations Report, Verizon
[x] http://www.csoonline.com/article/3136323/leadership-management/healthcare-industry-is-the-bullseye-for-hackers-in-2017.html
[xi] http://www.csoonline.com/article/3136323/leadership-management/healthcare-industry-is-the-bullseye-for-hackers-in-2017.html
[xii] https://www.healthitoutcomes.com/doc/healthcare-continues-to-be-top-cyber-attack-target-0001
[xiii] http://www.zdnet.com/article/ransomware-these-four-industries-are-the-most-frequently-attacked/
[xiv] https://blogs.forcepoint.com/security-labs/shelf-ransomware-used-target-healthcare-sector
[xv] http://www.modernhealthcare.com/article/20160330/NEWS/160339997
[xvi] http://www.networkworld.com/article/3011103/security/biggest-data-breaches-of-2015.html
[xvii] http://www.networkworld.com/article/3192885/healthcare/healthcare-data-breaches-skyrocket-but-is-there-good-news-coming.html
[xviii] http://www.cnbc.com/2017/03/14/verizon-sought-925-million-discount-for-yahoo-merger-got-350-million.html
[xix] http://www.zdnet.com/article/most-us-firms-would-pay-to-avoid-data-breach-shame-going-public/
[xx] http://www.bbc.com/news/uk-39918426
[xxi] http://www.securedgenetworks.com/blog/healthcare-ransomware-the-threat-you-should-be-concerned-about
[xxii] http://www.websense.com/assets/reports/report-2015-industry-drill-down-healthcare-en.pdf
[xxiii] http://www.csoonline.com/article/3136323/leadership-management/healthcare-industry-is-the-bullseye-for-hackers-in-2017.html
[xxiv] http://www.networkworld.com/article/3192885/healthcare/healthcare-data-breaches-skyrocket-but-is-there-good-news-coming.html
[xxv] http://www.networkworld.com/article/3168401/security/hospital-devices-left-vulnerable-leave-patients-vulnerable.html
[xxvi] Source: *2017 Data Breach Investigations Report*, Verizon