FOCUS HITECH—PRIVACY & SECURITY ISSUES

Healthcare Information Security

A Focus on Prevention Is the Best Remedy for Medical Record Breaches

By Keith Tyson and Robert Slocum

ABSTRACT

Between 2009 and 2011, more than 18 million patients' Protected Health Information (PHI) was compromised.[2] Over the past year alone, healthcare breaches in the United States have increased by 32 percent.[3] As these numbers clearly show, securing medical information is one of the most pressing issues facing hospitals and other healthcare organizations. However, a 2012 report from the American National Standards Institute notes, a lack of resources and leadership support have made it hard for many organizations to effectively protect such data.[1] In recent Dell SecureWorks roundtables with health IT executives, almost all participants personally knew of an organization that had experienced a PHI (protected health information) breach. Several admitted to experiencing a breach themselves in the past year. As responses at these roundtable events indicate, health IT executives are very aware of security concerns, but many obstacles make it difficult for them to seamlessly implement a security program that works on both a technical and human level.This challenge creates a "perfect storm" of risk, resulting in penalties and fines that have already exceeded $1.5 million per facility, per breach.[4] Experts estimate that costs to the healthcare industry could total more than $6.5 billion per year.[5]

With the implementation of basic controls and measures, however, healthcare organizations can effectively reduce the majority of their risk. A critical first step toward building a robust security program is conducting a comprehensive risk assessment, along with implementing stronger controls and cost-effective technologies. This paper explores the trends driving the need for more comprehensive security programs while continuing to embrace new technology, and why an approach that incorporates factors such as mobile devices is critical for positive change throughout the healthcare security ecosystem. By laying a solid foundation for security that includes visibility into an organization's vulnerabilities, encryption, endpoint access security, mobile device strategies and security risk monitoring, healthcare organizations can effectively address malware risk and data loss, enable better response to a threat environment that is rapidly evolving, and more efficiently meet compliance requirements.

KEYWORDS

Healthcare data security, information security, healthcare compliance, healthcare data management, data breach management, HIPAA security compliance, mobile device security, managed security.

HEALTHCARE DATA security has become a primary concern for firms of all types, from providers and business partners, to clinical research organizations. Within a "perfect storm" of looming federal audits, new penalties under the Meaningful Use incentive program, and risk of public exposure resulting from the federal Breach Notification Rule, organizations that have not properly planned for and understood security risks are facing increased public scrutiny. However, in the barrage of priorities, security often takes second place to issues such as budget concerns and patient care initiatives. In Dell-moderated, security-focused discussions with health IT leaders, participants conveyed an environment in which the magnitude of threats is difficult to assess. A number of participants also expressed concern about the low level of commitment in their organizations to improving information security, and several said that management and clinical leaders were often at odds on the issue.[6]

Developing an effective and efficient defense against external and internal attacks requires a high level of situational awareness and comprehensive controls. The attacks themselves have become increasingly sophisticated and evolved, with increased points of entry for hackers, but there are simple and powerful steps healthcare organizations can take to greatly minimize the magnitude of these risks. By conducting periodic risk assessments, enabling endpoint access security, developing a monitoring and security mitigation plan, and implementing a mobile device strategy, healthcare companies can help protect themselves against the vast majority of the threats they face, and for far less than the cost of an average breach.

A critical starting point for effective security is visibility—visibility into where data resides, and visibility into what the real risks are. Stronger controls and cost-effective technologies, if integrated into an organization's core operational expenditure investments, can also provide relatively inexpensive protection of the data perimeter and beyond, and address risk and response measures, without the need to pursue increasingly sophisticated technologies.

THE RISK LANDSCAPE

It is no secret that healthcare has faced increasing risks to PHI, relative to other industries. These risks are driven partially by the adoption of electronic health records (EHR), and increasing interconnectedness within and among institutions through the adoption of mobile devices and the rollout of health information exchanges. The incentives for healthcare companies to rapidly adopt EHRs are in place, as are disincentives for losing sight of data security in the process.

In fact, the American Recovery and Reinvestment Act of 2009 (ARRA) has breathed unprecedented life into the quest for electronic information, with providers eligible to receive up to $27 billion overall in incentive funds for the meaningful use of EHRs.[7] In addition to the incentives, healthcare providers also could face reductions in Medicare reimbursement if they do not comply with the legislation's Meaningful Use standards by 2015.

Despite these incentives, more than 18 million patients' records were breached between 2009 and 2011,[8] with an increase of 32 percent from 2010 to 2011; which could be costing the healthcare industry an average $6.5 billion per year.[9] More unsettling, a December 2011 study from the Ponemon Institute indicated that 96 percent of healthcare providers had at least one data breach in the past two years,[10] and *Information Week* reported that two of the top six data breaches of 2011 were healthcare-related.[11] This trend is likely occurring because 69 percent of hospitals do not have the proper policies and controls to detect and respond to breaches.[12]

Ironically, despite incentives for implementing secure EHRs, and the growing disincentives for maintaining the status quo, healthcare leaders have yet to allocate significant capital budgets to security initiatives. Of eight major industries, healthcare organizations spend by far the least per employee on security. The financial industry spends more than *six times* per employee on security than do healthcare organizations.[13] When this spending is compared to the overall costs of a breach,[14] healthcare again lands at the bottom rung of the preparedness ladder (**Figure 1**). This indicates that not only are healthcare providers reluctant to spend money on security; they are one of the industries that would ideally spend the most to gain a firm security posture based on a higher risk profile than most industries.

To gain a broader perspective on these risks, Dell conducted focus groups with more than 100 health IT executives to learn the most prevalent and concerning threats they face. Almost all participants were personally acquainted with an organization that has had a breach of ePHI, and some said they had experienced a breach themselves in

FIGURE 1: Spending Compared to the Overall Costs of a Breach

	Security Spend per Employee*	Breach Costs per Employee**	Spend/Cost
Financial	$904	$247	366%
Professional Services	$665	$185	359%
Communications	$995	$334	298%
Education	$298	$142	210%
Transportation	$308	$196	157%
Retail	$253	$174	145%
Industrial	$237	$235	101%
Healthcare	**$145**	**$240**	**60%**
	Last on List	Top-3	

* Source: Gartner, IT Metrics Data 2012: Key Information Security Measures – by Industry (12-2011)

** Source: Ponemon, Cost of a Data Breach Study (2011) (US only) (03-2012)

A CRITICAL FIRST STEP toward building a robust security program is conducting a comprehensive risk assessment, along with implementing stronger controls and cost-effective technologies.

the past year. As responses at these roundtable events indicate, awareness of security concerns is high, but many obstacles make it difficult to seamlessly implement a security program that works on both a technical and human level. The typical approach is primarily symptomatic and reactionary. Frameworks, if they are adopted, are often an incomplete work in progress.

Event participants noted that they typically spend less time evaluating new solutions than they do trying to plug holes in existing systems, while struggling to maintain visibility into emerging advanced threats and other malware risks. Hospitals have difficulty keeping common malware out of their networks, but ironically, they frequently de-prioritize security due to a perceived immunity to breaches. While health organizations may have a security strategy, they are typically limited in scope.

INTERNAL VS. EXTERNAL THREATS

Although the risks facing healthcare organizations surface from both internal and external sources, internal threats have historically been the most common, with a reported 49 percent of breaches occurring due to lost or stolen devices and laptops.[15] The prominent media image of a healthcare breach often evokes the occasional rogue employee who steals information and sells it on the black market. In fact, most healthcare security incidents result from more mundane and unintended causes, such as the accidental loss or theft of laptop computers or mobile devices: a clinician or employee leaves a laptop or mobile device on a train during their evening commute; or a thief steals an employee's computer bag from the backseat of her car. Situations such as these create an easy opportunity for thieves whose target may be the hardware itself (and not the data on the device); but once the device is stolen, the repercussions are similar, regardless of the intent.

The *external* threat landscape, however, is also a force with which to be reckoned, and presents its own unique set of challenges for the IT security professional. Recent attacks perpetrated against many industries are highly sophisticated, well organized, and often are connected to nation-state activities or cyber-crime organizations around the globe. The actors behind these attacks are sometimes not motivated as much by recognition or fame, as they are by monetary, political or ideological objective.

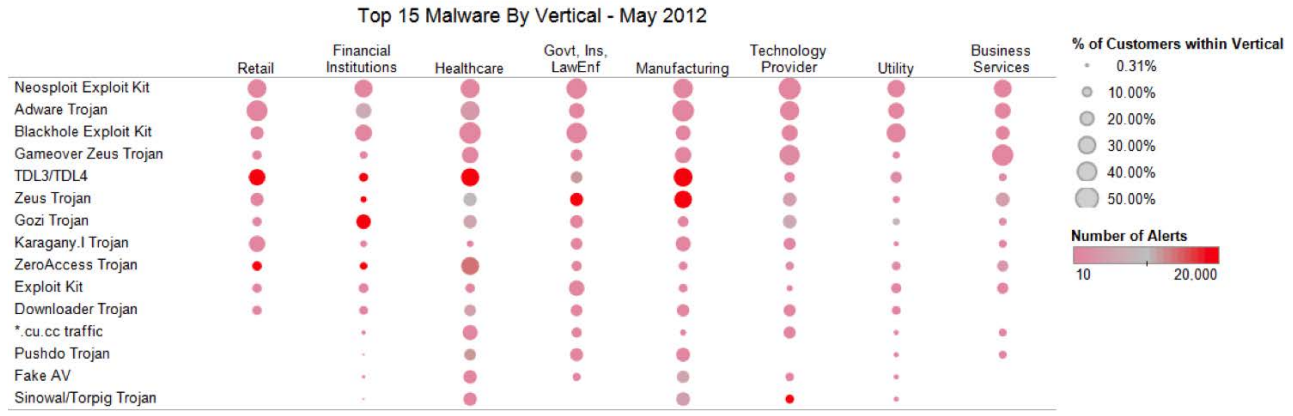
One of the most insidious types of attacks is advanced persistent threats (APT), a genre with generally malicious intent that greatly compounds the risks inherent in EHRs. This type of attack represents an evolving threat to many organizations' intellectual property, financial assets, and ultimately, their reputations. APT actors (the adversaries guiding the attack) target specific organizations for a singular purpose, and attempt to gain a foothold in the target's environment, often through tactics such as targeted emails, or "spear-phishing," that contain malicious web links or attachments designed to compromise a particular computer. The attackers then typically use the compromised systems as a conduit into the target network and as a method to deploy additional tools that help fulfill their primary objectives. Dell SecureWorks' Counter Threat Unit has found that the healthcare industry is particularly vulnerable in recent months, with many of the most prevalent malware tools used by hackers (**Figure 2**). This may be partially due to the attackers' strategy of using healthcare organizations as a "testing ground" for malware, before deploying it on targets in other industries. Healthcare organizations are viable testing platforms for "proof of concept" attacks, due to the general lack of effective controls and high state of vulnerability throughout their networks.

Organizations can protect against both common and advanced threats by gaining situational awareness, and forming defensive strategies around the risk posture that exists. Although a foundation for this awareness starts with risk assessments, implementing effective network architecture, along with penetration testing and continuous monitoring are also necessary components of a security program. Planning for these events and the organization's anticipated response on a continual basis makes it much more difficult for malware actors to conceal their actions, and will make incident response efforts more effective, both for internally- and externally-based threats.

DATA VISIBILITY AND RISK ASSESSMENTS

Gaining visibility into where data resides is a critical starting point to developing a robust security strategy, and is the basis for the completion of a comprehensive risk assessment. Conducting a risk assessment as a foundation for IT strategy helps the organization meet compliance requirements such as HIPAA and Meaningful Use, but is also a substantial step in creating the capability to react to and mitigate the damage from breaches. These breaches, unfortunately, are an increasing likelihood with the proliferation of EHR implementations and recent spikes in device usage. Having a comprehensive picture of where data is, how it is used, and who is accessing it goes a long way toward maintaining integrity of patient records, preventing negative press,

FIGURE 2: Top 15 Malware by Vertical—May 2012



Source: Dell SecureWorks' Counter Threat Unit (CTU) analysis

and avoiding substantial fines and penalties. A risk assessment and analysis is also the primary starting point for two of the primary concerns in healthcare today—securing mobile devices and meeting the Stage I security requirement for meaningful use of EHR.

Organizations participating in the EHR Meaningful Use program already have a compelling incentive to conduct or update a security risk analysis, since this is a core requirement of both Meaningful Use and the original HIPAA Security Rule. However, simply pushing the organization to meet Meaningful Use with the singular goal of collecting incentive payouts does not prepare the organization for inevitable future audits and to mitigate the additional risks posed by online data access, mobile devices, health information exchanges, accountable care organizations, increased abilities of hackers, and the increased demands from macroeconomic trends such as aging of the population.

There are fundamental components of any assessment that healthcare organizations need to consider to address these emerging risks: understanding what controls are currently in effect, determining the impact of likely events from viruses to natural disasters, and documenting exposures and vulnerabilities; not only in systems, but also in processes. A healthcare organization's assessment program should consider the controls that are implemented to safeguard the systems and information, and the physical facility and surrounding environment as well.

MOBILE DEVICE SECURITY

Simultaneous with the expected growth of EHRs is the rapid emergence of mobile devices such as smartphones and tablets. The proliferation of such tools indicates that many of the "test flights" for EHRs will be driven by these devices, which combine potential improvements with new risks. The widespread use of portable media, smartphones, and tablet computers creates an urgent need for attention to how and where sensitive data is sent within (and outside of) the provider's networks.

A changing relationship with how and where physicians, clinicians, insurers, and billers access information is complicating the list of vulnerabilities that providers face. Handheld devices are particularly notable because these devices put more power in the palm of the hand today than a desktop PC had just a few years ago.[16] Moreover, clinicians have taken notice: more than 70 percent of U.S. physicians now use smartphones, up from just 30 percent of physicians in 2001.[17] In addition, some 39 percent of Chief Medical Information Officers have rolled out mobile computers or handhelds at their facilities (as of 2011)[18], and 86 percent of physicians express that their top interest in mobile technology is for accessing electronic medical records.[19]

In many cases, both employees and patients can use unsecured personal devices to carry or access health information (often referred to as the "bring-your-own-device," or BYOD movement), which brings into question the ability to consistently enforce security controls such as encryption, and track access to appropriate data. The unforeseen consequences from this can be significant. In recent months for instance, a US health insurance firm lost 1.5 million clients' medical records on an unencrypted portable drive. This decision to save money on encryption expenses resulted in $250,000 fielding lawsuits, more than $319,000 in letters to the affected clients, and $1 million for identity theft monitoring services to the victims.[20] Although BYOD can be a beneficial recruiting tool and can enable an organization to lower its IT acquisition costs, the risks inherent in this trend (taken without adequate controls in place) cannot be overstated.

The damage from breaches due to mobile devices also costs the most to repair. A standard USB drive can store more than 25,000 medical records, and losing just one such device can cost an organization more than $5.7 million in breach mitigation costs.[21] On average, each record breached involving a mobile device can amount to $258 in mitigation costs, which is higher than the costs associated with other causes of breaches.[22] When considered in the context that hard drives can carry and manage more data with each passing year, there is

a clear imperative to implement a strategy for each device that touches the organization's network.

To fully manage security in a mobile environment, organizations need to ask themselves several key questions to gain insight into who is accessing their data and what types of controls are in place. They also must consider information security best practices as a part of the overall mobile technology and security strategy. For instance, both enterprise-integrated mobile devices and employee- or patient-owned mobile devices need to be as secure as possible with identity authentication, encryption, tracking and trace software, anti-malware, backup and extensive monitoring.

Access controls must be implemented to keep data safe in the mobile environment. The original HIPAA rule called for granting role-based access procedures. But as mobile device usage has required identities and privileges to be stored in multiple applications and repositories across the enterprise, many current systems may have deficiencies in this area. A centralized and comprehensive view of people, views, roles, and privileges is necessary to enable more accurate and efficient auditing and reporting.

Another critical challenge in keeping mobile devices secure is the threat posed by personal applications for social media and games, which are often installed directly adjacent to work applications. To address this risk, a "container approach" to application development and deployment is necessary in order to separate the high-risk personal applications from work applications on the same device.

Remote wiping capability, another common requirement among mobile device users, allows organizations to address those instances where work applications residing on an individual's mobile device need to be erased without affecting their personal applications; thus eliminating potential threats when a device is lost or an employee leaves the organization.

ENDPOINT ACCESS AND ENCRYPTION

Endpoint security has become a larger imperative as healthcare providers continuously move toward adoption of electronic medical records. Compliance officers and IT staffs are challenged with giving clinicians single-sign-on for immediate access to patient records, while simultaneously keeping the data secure. Single-sign-on capabilities allow for seamless session transfer, which improves the speed of access to patient records, while reducing the risk posed from unauthorized employees accessing patient data that they may not have a need to view.

An example of endpoint management is Dell's Mobile Clinical Computing solution, which uses client virtualization – a solution that removes data including ePHI from endpoint devices. Coupled with single-sign-on capabilities, solutions such as this allow clinicians to move from their office, then to a nursing station or a patient room, while logging onto devices via a card reader, facial scan, or thumb reader. Upon logging on, the record or image follows the clinician virtually, while automatically logging them off any other systems onto which they may have been logged. With each endpoint or "thin client" being virtualized, there are no data or patient records residing on an individual client device. The endpoints in these cases are simply "gateways" to data. If an employee walks out with a laptop or thin client, there is no data loss; and without logon credentials, there is no way for them to access the medical records.

For those systems that do contain records or data, encryption is necessary. Historically, encryption was performed at the hard drive layer, subsequently slowing down the workstation or server, which in turn impeded physicians from expediently accessing medical records. As backlash ensued, IT managers often turned off the encryption completely to assuage the problems with patient data access. Even those who did not disable encryption were still exposed to breaches at the USB ports and optical drives. Today, encryption methods have evolved, and affordable systems are available that meet the stringent FIPS 140-2 level-three encryption standards at the system level. These advancements encrypt the entire system, including USB and optical drives without impacting the system's performance or patient record access speed.

DATA CENTER AND NETWORKING SECURITY

As another layer of defense, data center and network security solutions directly address malware. Malware is typically presented in three various forms, or vectors: internal web threats, external web threats, and spam and virus via email attachments. The end goal of malware actors is typically to entice a victim to click on a link or website which contains malware, and can subsequently allow the actor entry to the data center and network; either to extract financial or patient data for monetary gain, or for other purposes in the case of advanced threats. Next Generation Firewalls and Web Application Firewalls can help shield the network and servers from external attacks; and intrusion prevention systems can bolster this defense. As an added layer of defense, installing a web filter can enable the organization to monitor the network and protect internal employees from picking up malware while browsing the internet. Anti-virus and anti-spam gateways can also provide protection from email-based attacks while providing an overall boost to performance by allowing the organization to reduce the volume of email traffic consisting of spam messages.

CONTINUOUS MONITORING

Since the volume and sophistication of malware is rising, it is imperative that healthcare organizations block threats across all communication layers—from the network to e-mail to applications. A solid platform for these appliances will provide labs to monitor and protect the organization against the current threats, but that protection is limited to that particular appliance. When evaluating their overall security strategy, many healthcare organizations scrutinize their budgets and try to fund an internal information security staff to examine current threats, monitor all the endpoint devices on a network, and monitor all of the security appliances running in front of their data center, in the hopes of staying ahead of evolving threats.

A new approach to security is to implement outside security monitoring. Monitoring services such as Dell SecureWorks enable healthcare organizations to assess security across the enterprise, from onsite access endpoints to mobile solutions, where their current and future infrastructure are continuously examined and disaster plans are created. Services such as these couple risk assessments with threat monitoring, and enable the organization to scale its security efforts, and monitor risks across the entire network. Real-time threat management keeps the organization secure, helps to meet compliance requirements, and allows the organization to focus budgets on those activities that deliver information-driven healthcare and enhance core patient care activities.

In the quest to improve patient outcomes, organizations need to embrace new innovations. As the cloud has continued to mature, more hospitals are embracing a cloud strategy to managing their data. This is evident in medical imaging, as healthcare organizations aspire to remove data silos, manage the data explosion that is driving health information exchanges and effectively confront accountable care organizations. To address the evolution in data exchange and sharing, organizations are recognizing that there is tangible value in coupling disaster recovery mechanisms with geographically separated data centers, along with fully integrated and around-the-clock security coverage.

CONCLUSION

A changing relationship with how and where physicians, clinicians, and billers access information is complicating the list of vulnerabilities that exist in the world of healthcare data management. In an environment where many security decisions are made based on compliance-driven and reactionary motives, organizations risk fighting an uphill battle to stay ahead of current threats, mitigate loss of patient and financial data, and maintain a continuous picture of their current state of risk. To more effectively deal with information security in the information age, healthcare providers need to make it a strategic pursuit. Instead of simply reacting to the call for compliance or the need to prevent or respond to a breach, healthcare leaders should adopt a more holistic approach. Along with a stronger alignment between administration, IT, and clinicians, more automation and better tools are necessary to manage a threat landscape that evolves at an ever-faster clip with each passing year.

Despite the introduction of new and varied threats with each passing month, healthcare providers can cost-effectively manage security with a layered approach that includes conducting risk assessments, managing mobile devices, applying encryption and endpoint controls, implementing data center and network security controls, and implementing continuous monitoring. Using this approach, healthcare organizations enable themselves to focus their human capital and core resources on pursuing and managing innovation that furthers the mission of improving patient outcomes. **JHIM**

Keith Tyson is a healthcare industry consultant with Dell SecureWorks. He has over 12 years of experience managing medical supplies development and commercialization, oncology program strategy, software innovation and development, and providing thought leadership to the data security community. He is a frequent blogger, writer, and speaker for Dell on security issues facing healthcare organizations. He holds an MBA from Emory University.

Robert Slocum is a sales and marketing professional with an extensive history leading, managing, coaching, marketing and selling in the high-tech, medical and financial industries. Slocum currently works in Dell's HealthCare and Life Sciences group, helping customers to meet IT Security, networking security, data protection and enterprise storage solutions. Slocum graduated Cum Laude from Concordia University.

REFERENCES

1. American National Standards Institute. The Financial Impact of Breached Protected Health Information: A Business Case for Enhanced PHI Security. 2012.
2. http://www.ama-assn.org/amednews/m/2012/04/02/bsf0405.htm
3. Second Annual Benchmark Study on Patient Privacy & Data Security. Ponemon Institute, December 2011
4. http://www.healthdatamanagement.com/news/breach-notification-hipaa-privacy-security-tennessee-44181-1.html
5. Second Annual Benchmark Study on Patient Privacy & Data Security," Ponemon Institute, December 2011
6. http://www.secureworks.com/assets/pdf-store/articles/healthcare_data_security_landscape_2012.pdf
7. http://healthit.hhs.gov/portal/server.pt?open=512&mode=2&objID=3541
8. http://www.ama-assn.org/amednews/m/2012/04/02/bsf0405.htm
9. Second Annual Benchmark Study on Patient Privacy & Data Security," Ponemon Institute, December 2011
10. *Ibid*.
11. http://www.informationweek.com/news/security/attacks/232301079
12. http://www2.idexpertscorp.com/press/new-ponemon-institute-study-finds-data-breaches-cost-hospitals-6-billion/
13. Gartner. IT Key Metrics Data 2012: Key Information Security Measures – by industry (12-2011)
14. Ponemon Institute, Cost of a Data Breach Study (2011) (US only) (03-2012)
15. http://www.informationweek.com/news/healthcare/mobile-wireless/232601422
16. http://bits.blogs.nytimes.com/2011/10/12/cell-phones-are-servers-and-servers-are-cell-phones/
17. Manhattan Research, "Taking the Pulse" Research Report 2011.
18. http://mobihealthnews.com/7985/cmios-39-percent-have-installed-mobile-devices/
19. PricewaterhouseCoopers Health Research Institute report: "Healthcare Unwired," September 2010.
20. http://www.forbes.com/sites/dell/2011/09/22/mobile-devices-in-healthcare/
21. Ibid.; SecureWorks research.
22. HITRUST Alliance. An Analysis of Breaches Affecting 500 or More Individuals in Healthcare.