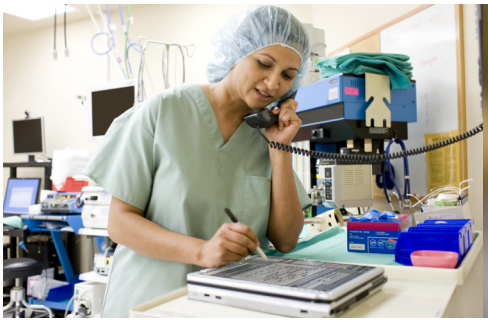
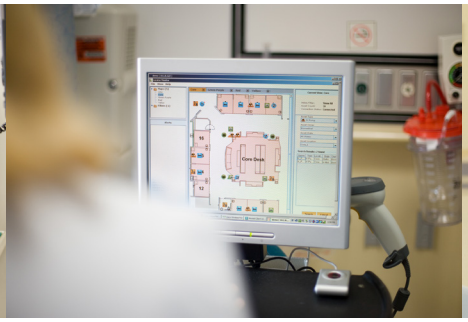
Combating Cybercrime in the Healthcare Industry

White Paper


Medical information costs 10 times more than credit card information on the black market.

—Thomson Reuters

Insights on Overcoming the Obstacles of Protecting Personal Healthcare Information

Healthcare security breaches are making headlines with escalating frequency. Consequently, the need to safeguard personal health information (PHI) and other nonpublic data looms more urgent with each passing day. Yet, healthcare organizations are unable to respond. They're currently starved of cash, thanks largely to declining Medicare and insurance reimbursements as well as the growing trend to pay by results rather than pay by procedures.

While recent developments shine an unsettling public spotlight on healthcare crime, to security experts in the industry, the concern goes far deeper than the mainstream news. A vast number of breaches aren't even reported. In fact, 80 percent of medical record thefts remain unnoticed for months, and sometimes years, according to Cisco® Security healthcare expert Richard Staynings.

Rise of Medical Records Theft

Healthcare security is a global issue, but the medical records of more than 40 million Americans were breached in 2014.[1] More than 50 percent of those were a result of cyberattacks. One attack alone exposed 4.5 million patient records. With the rising value of health records on the black market—roughly 10 times that of other records—it was only a matter of time before hackers began targeting hospitals and healthcare organizations in general.

The Ponemon Institute conducted a security survey of patients treated during 2014.[2] What they discovered is startling. Medical identity theft increased by nearly 22 percent. This amounts to an estimated US$12 billion annual unbudgeted cost to the healthcare industry further compounding existing budgetary pressures. Of the theft victims, 50 percent do nothing. Many who attempt to resolve the incidents spend over 200 hours doing so. 65 percent of the victims pay healthcare providers, insurers, identity services, and lawyers with their own money, with the average costs totaling $13,450 in order to resolve these issues.

1. Redspin Issues *Annual Healthcare Data Breach Report*, February 24, 2015
2. *The Top U.S. Healthcare Story For 2014: Cybersecurity*, Forbes, December 21, 2014

As a result, healthcare organizations are now intensely focused on the sheer volume of PHI they maintain. "They are reducing how much unprotected PHI they store to make themselves appear less attractive to hackers and to decrease the risk of exposing patients to medical identity fraud. This isn't a security measure, it's a survival instinct." Says Todd Feinman, chief executive officer, Identity Finder LLC.

ABI Research calculates that healthcare's cybersecurity spending will reach only $10 billion globally by 2020.[3]

Funding Dilemma

The problem is compounded by the fact that the healthcare industry doesn't view cybersecurity to be as much of a strategic priority as the finance and defense industries do. Healthcare funding is focused squarely on the human and technology assets that make medical treatment possible. Information security is largely an after-thought, or viewed simply as a 'cost of doing business', rather than as 'business-enabler' to permit healthcare organizations to expand their services into lucrative new revenue streams or more efficient ways of conducting existing business. ABI Research calculates that healthcare's cybersecurity spending will reach only $10 billion globally by 2020.[3] That amounts to less than 10 percent of global spending on critical infrastructure security.

Dire Talent Shortage

A lack of money is only part of the problem. Locating the right security talent is equally challenging, and the hunt for qualified candidates is only becoming more difficult. Government estimates put the total of available cybersecurity jobs at 210,000.[4] "It's probably 10 to 12 times harder to find cybersecurity professionals than it is to find general IT professionals," says Rashesh Jethi, director, Cisco Security Services Group. Even if you can find qualified professionals, keeping them is another story, particularly high-level security talent. Ponemon Institute research indicates that chief information security officers (CISOs), and other senior security executives, leave their jobs on average after just two and a half years.[5]

Meanwhile, job-opening numbers continue to climb higher. Cybersecurity postings grew 74 percent between 2007 and 2013, a growth rate double that of all other IT jobs. The openings take 24 percent longer to fill than other IT job postings. In short, the demand for cybersecurity talent appears to be quickly outpacing supply. In the United States alone, employers posted 50,000 jobs requesting Certified Information Systems Security Professionals (CISSPs). The country's entire pool of CISSPs totals just 60,000.

3. *Healthcare Cybersecurity a Massive Concern as Spending Set to Reach Only US$10 Billion by 2020*, ABI Research, February 25, 2015
4. Remarks from Commerce Secretary Penny Pritzker on *Training America's Workforce* at Montgomery College, December 10, 2014
5. *Understaffed and at Risk: Today's IT Security Department*, Ponemon Institute sponsored by HP Enterprise Security, February 2014

The demand is so high that cybersecurity jobs pay an average of $15,000 more than similar nonsecurity IT jobs.[6]

The issue for healthcare organizations is not just attracting security talent, but retaining it. With such a shortage of security professionals nationally, other more cash-rich industries are sending their recruiters after the experienced security talent in healthcare and luring many of them away with attractive salaries, stock grants and options, large bonuses, and other benefits.

Despite all obstacles, healthcare organizations can use practical means to address their cybersecurity challenges.

Table 1 IT Security Salaries

Position	2014	2015	Comparison to 2014 Salaries
Chief security officer	$126,250 - $208,000	$138,000 to $219,750	up 7.0 percent
Data security analyst	$100,500 - $137,250	$106,250 - $149,000	up 7.4 percent
Systems security administrator	$ 95,250 - $131,500	$100,000 - $140,250	up 6 percent
Network security administrator	$ 95,000 - $130,750	$99,250 - $138,500	up 5.3 percent
Network security engineer	$ 99,750 - $131,250	$105,000 - $141,500	up 6.7 percent
Information systems security manager	$115,250 - $160,000	$122,250 - $171,250	up 6.6 percent

New Era of Managed Solutions

Despite all obstacles, healthcare organizations can use practical means to address their cybersecurity challenges. Managed solutions demand less infrastructure and fewer people to oversee their operations, and can complement overall information security goals. They're agile, easy to scale, and allow internal security teams to focus their time on strategic initiatives and higher value security tasks. Managed solutions often employ advanced technology that requires little experimentation. "It's not just a question of cost savings and access to advanced security technology," says Staynings, "you're gaining access to top security talent and expertise that you could never afford yourself as a healthcare institution." Managed solutions are not a panacea, but they can assist healthcare providers to quickly move to the next level of security defenses without the need to hire additional staff and spin-up a two or three year long project to get there.

6. *Job Market Intelligence: Report on the Growth of Cybersecurity Jobs*, Burning Glass, March 2014

Employing analytics is absolutely indispensable. Cybercriminals are continually gathering intelligence on security solutions, so they can assume less-visible behavioral patterns to better conceal their actions.

Some healthcare organizations may be reluctant to adopt managed solutions due to compliance concerns. But those concerns are now being addressed. Major cloud service providers offer reliable, scalable, affordable solutions that meet regulatory requirements. Many healthcare CISOs are slowly coming to the realization that their data is often better protected in the cloud than in their own understaffed and underfunded data centers. Cloud providers have had to invest heavily in security to overcome customer concerns, and employ the very best security tools and well-equipped and trained security staffs. That's not to say that cloud-based services are infallible, but that they are often better protected than those still run from hospital data centers.

As cost pressures force healthcare CIOs to move more of their applications to the cloud, the complexity of securing healthcare data has increased. This is leading to a re-evaluation of the focus of healthcare security teams from a labor-intensive, operational basis, to smaller agile teams of professionals supported by improved technologies, and security services provided by vendors with the expertise to manage increasingly complex solutions to ever-evolving security problems.

Insight No. 1: Big data and analytics are essential for making informed, strategic security decisions. Their importance will only grow in the future.

Security information event management (SIEM) has been the traditional solution used in data centers. However, SIEMs are being overwhelmed by the large volumes of incoming data. These database systems are only as good as the people who operate them and the information they retrieve. Such mountains of data, without intelligent analytics, and knowledgeable security professionals, are fundamentally useless.

Employing analytics is absolutely indispensable. Cybercriminals are continually gathering intelligence on security solutions, so they can assume less-visible behavioral patterns to better conceal their actions. Data must therefore be analyzed quickly to identify actionable insights and keep attackers at bay. Big data and analytics convert unstructured log and SIEM data to a format that enables informed, strategic decision making, and does away with the 'false-positives' that afflict SIEMS. This allows security teams to quickly respond to threats before data leaves the network.

Insight No. 2: Your own employees often are your organization's biggest vulnerability.

Security professionals generally assume employees will click on anything, regardless of what they're told. They have to, because users are the main entry point for the majority of network breaches. And while 75 percent of attacks take only minutes to begin data exfiltration, they take much longer to detect. More than 50 percent of all breachs go months before being detected. After these attacks are discovered, they take several weeks to contain and remediate.[7]

7. *The Top U.S. Healthcare Story For 2014: Cybersecurity,* Forbes, December 21, 2014

Securing email and web gateways prevents employees from hurting their organizations. This includes rewriting or sandboxing suspicious URLs to detect drive-by attacks and by deploying authentication, endpoint, network, and gateway controls that share information for an orchestrated reduction on the attack surface. Other measures include implementing a solid supply chain and vendor management system, promoting education training awareness (ETA), reducing access control lists (ACLs), and knowing what key intellectual property exists on the network and where it's located.

For example, 98 percent of applications written for the Android platform contain gaping security vulnerabilities. These unsafe practices are widespread, and IT departments rarely have the time or the resources to do anything to mitigate them.

Insight No. 3: BYOD has reached epidemic proportions in the healthcare industry.

Bring-your-own-device (BYOD) programs are a huge concern for many healthcare organizations, because people prefer using their Apple MacBooks and iPads, Android tablets, and smartphones. Staff, physicians, and even senior executives who know the risks often refuse to use their standard Windows laptops for official business functions. In addition, the mobile applications that employees install and use on their personal devices expose corporate IT to additional risks. For example, 98 percent of applications written for the Android platform contain gaping security vulnerabilities. These unsafe practices are widespread, and IT departments rarely have the time or the resources to do anything to mitigate them. Many healthcare organizations lack even the most basic mobile device management (MDM) or BYOD tools, policies, and processes.

BYOD and mobile threats change almost constantly due to the proliferation of new mobile applications being written. Healthcare organizations need to implement adaptive technologies to manage identities and to better control the data being accessed, and the method by which it is accessed. Next generation identity tools like Cisco's Identity Services Engine (ISE) can greatly assist in managing these risks.

Insight No. 4: Networks need to operate as sensors, with all security devices communicating to provide actionable intelligence.

Simply deploying best-of-breed solutions doesn't work anymore. To neutralize sophisticated threats, a network's visibility, intelligence, and response capabilities must be coordinated. Security information now needs to be shared by all of the security products and solutions throughout the network and Cisco is investing considerable resources to see that happen. Its solutions are designed to work together with partner solutions in a way that allows the entire network infrastructure to function as a sensor, so that visibility, detection, containment, and mitigation are all successful.

Insight No. 5: Failing to properly secure personal healthcare information can be costly.

If a personal credit card is compromised, the bank assumes the loss, issues a new card number, and life goes on. When a person's healthcare information is compromised there is no quick fix. You cannot un-ring the bell. Information such as addresses, Social Security Numbers, and medical histories are much more static than credit cards and contain information that most people would want to keep private. Just look at what some of the tabloids have paid for the partial medical information of celebrities over the years. This information can be used in a multitude of ways to harm and exploit the individuals over a much longer span of time. If a victim's blood type or allergies are changed in their health records the result could be life threatening. This is happening every day now as medical identity theft results in many people sharing the same insurance and medical record.

Today's medical records contain so much information that they make a very lucrative target for hackers.

Medical identity theft is now highly organized. Hackers have specialized into groups, or actual companies in many cases, of vulnerability finders, exploit writers, and exploit executers who then exfiltrate medical and personal information from poorly protected healthcare networks. There's a vibrant trade in the production and sale of exploit kits and other hacking tools that is growing at an alarming pace out of sight of law enforcement. It's an international problem that current law enforcement is ill-positioned to tackle. Once a medical record has been exfiltrated from a health system, it is parsed into its component parts where cyber thieves can make much more money. Personal identities are sold to identity theft groups, medical insurance information sold on the black market to those without insurance, credit card, and banking information from billing records is sold to other groups who then go about emptying bank accounts and running up credit card bills, records of confidential medical procedures are sold to the highest bidder for publication or blackmail. The possibilities go on. Today's medical records contain so much information that they make a very lucrative target for hackers.

The cost of loss for providers, payers, and other HIPAA covered entities can be huge. Fines from state agencies for privacy breach, expensive investigations by OCR HSS and subsequent further fines for regulatory breach, expensive and time consuming internal investigation and remediation, and then there's the class action lawsuit. These have grown in size to reach the annual GDP of small countries. They are not just the death-knell for smaller organizations without adequate insurance; they are a potential extinction event for covered entities across large parts of the United States. Imagine having to drive 300 miles to get to a hospital because everything closer went out of business and closed because of data breach. It's not as far off as you may think.

Combating Cybercrime in the Healthcare Industry

White Paper

Conclusion

With the high value of PHI records, and insufficient protection for them, healthcare organizations remain attractive targets for cybercriminals. The frequency of attacks will likely rise, and the financial and legal consequences will become more damaging. With no immediate answers in sight for healthcare's tight security budgets and the limited IT security talent pool, managed security providers are an ideal partnership for many healthcare related businesses. They can address existing security gaps quickly, provide customized solutions, and align with these organizations' businesses. Managed solutions deliver many benefits ideally suited for healthcare security concerns and deserve a closer look from any organization ready to address the challenges that lie ahead.

Read more about security in the healthcare industry and Cisco Security Services at www.cisco.com/go/securityservices.

DEC15CS4717 04/15