ENTERPRISE SECURITY IN HEALTHCARE: FROM CYBERCOMPLIANCE TO CYBERCONFIDENCE

ENTERPRISE SECURITY IN HEALTHCARE: FROM CYBERCOMPLIANCE TO CYBERCONFIDENCE

Global Institute for Emerging Healthcare Practices

Keeping up with ever-changing cyber threats is a challenge. New vulnerabilities related to mobile devices, portable media and medical devices give cybercriminals the opportunity to commit financial theft, identity theft, or cause malicious damage to equipment.

To stay ahead of criminals and ensure the protection of patient data, it is critical for organizations to view security not as a routine matter of protecting privacy or confidentiality. Organizations need to conduct a comprehensive risk assessment to combat outside threats, and if necessary, enlist the help of experts such as managed security service providers in order to secure their health IT environment.

Security is complicated, but it need not hinder an organization's growth or prevent it from using data assets to improve care delivery, quality and financial performance. With increased vigilance and the right technological tools, it is possible for healthcare organizations to achieve true cyberconfidence.

Cyber crime and data breaches are among the most commonly cited things that keep healthcare CIOs up at night. Given the level of preparedness that many organizations have today, this is not surprising.

Recent surveys show that roughly three quarters of healthcare organizations have suffered some kind of data breach or security incident in the past 12 months. Among small healthcare organizations (with 250 employees or fewer), the figure is an astonishing 91%.[1] According to the Department of Health and Human Services, over 19 million people have had their health information compromised since the breach notification rule went into effect just a few years ago.

Under the HITECH Act, hospitals and other organizations can be fined up to $1.5 million per year for serious security incidents, but the full cost of a breach goes far beyond the fines. According to one study, the cost of identifying and notifying affected individuals — now mandatory under the law — costs on average $214 per record.[2] Of course, there are also the intangible costs associated with compromised trust and reputation.

Breaches can lead to worse problems. Almost a quarter of healthcare organizations report experiencing at least one patient medical identity theft in the past year. The annual economic impact of medical identity theft is estimated at $41.3 billion, or an average cost per victim of $22,346. For healthcare facilities, the average settlement cost of a medical identity case is over $250,000.[3]

To protect against cyber threats, it is critical for organizations to view security not merely as a matter of protecting privacy or confidentiality. Cybercrime is on the rise as criminals search for new opportunities to commit financial theft, identity theft, or cause malicious damage to sensitive medical equipment.

With so many important initiatives underway and so few resources to tap, hospitals and other healthcare organizations have traditionally focused more on compliance with state and federal security than pursuing a truly robust, integrated, enterprise-type approach to ensuring the security of data and other key assets. When addressing privacy, organizations often measure themselves against HIPAA and patient feedback. For security, they measure themselves against HIPAA and the HITECH Act. These benchmarks, however, provide only basic guidance and are often vague.

The annual economic impact of medical identity theft is estimated at $41.3 billion, or an average cost per victim of $22,346.

Source: "Third Annual Survey on Medical Identity Theft" Ponemon Institute, June 2012

Federal and state laws governing healthcare IT security should be taken as a floor for capabilities, not a ceiling. While it may have been acceptable to make momentary cybercompliance a goal in the past, today's hospitals are finding that, to maximize security and performance, they need something much better: *persistent cyberconfidence.*

Most hackers who infiltrate health IT systems are seeking financial data, not medical information. In an analysis of 855 data breaches involving more than 174 million records from the health care, financial services, retail and hospitality industries, researchers recently found that such breaches are "almost entirely the work of financially motivated organized criminal groups, which typically attack smaller, low-risk targets to obtain personal and payment data for various fraud schemes."

Source: "2012 Data Breach Investigations Report" Verizon Communications, October 2012

Every Part of the Health IT Environment Needs to Be Secure

Security concerns are sometimes thought of as being driven by the adoption of electronic health records (EHR), the rise of health information exchanges, the pressure to improve quality and safety, the increased mobility of data and devices, and other issues. Having a secure health IT environment is essential to the success of all of these things, but it is not automatic and it cannot be taken for granted.

Hackers and cybercriminals will go after valuable information wherever it resides. Typically, cybercriminals do not distinguish based on public versus private sector, type of institution or other such factors.[4] Academic medical centers, community hospitals and rural physician practices are just as susceptible as any other organization. Experts believe, though, that as more large organizations address their security gaps, the majority of breaches will begin to come from smaller organizations and business associates.[5] These include small hospitals, as well as entities like transcriptionists, small outsourced radiologists, pharmacies and even small pharmaceutical companies.

Any misconfigured application or unmonitored spoke of a network can serve as a potential source of entry. It does not matter *how* a cybercriminal gains access to a system — it only matters *whether* they can and what information they can gain access to. Attackers target the most valuable information, and sell it to the highest bidder. On today's black market, a stolen medical identity has a street value of $50, compared to $14-18 for a credit card number or $1 for a social security number.[6] [7] Cybercrime is well-organized. Known websites and forums — many of which are in Russia — serve as marketplaces for records, data and information about exploits.

The Hotspots of Risk Are Always Changing

There are several different categories of risk. Some cybercriminals seek personal information in order to commit identity theft, insurance fraud, or financial theft. There are also patient safety risks from cybercriminals who steal and modify medical records, or that inject malware or software viruses into medical equipment.

In order to commit these types of theft, fraud, and malicious acts, cybercriminals constantly target new areas of perceived weakness. Three of the newest trouble areas for healthcare organizations are mobile devices, portable media and medical devices.

Mobile Devices

Mobile devices are a target for cybercriminals interested primarily in identity theft and financial theft. Although most breaches still come from laptops and paper records, breaches related to mobile devices are rising the fastest. Malicious files can spread much more quickly when large numbers of unmanaged devices are plugged into the same network.[8] The high level of mobility and small physical size of the assets also makes them good candidates for be stolen or lost.[9] According to a recent survey of IT executives, 57% of respondents named mobile clients and unmanaged devices their top security challenge.[10]

Common problems and concerns surrounding mobile devices include:

- Mobile devices frequently do not have strong passwords, and/or authentication is disabled
- The operating systems of mobile devices were not designed to be secure
- Devices can easily be lost
- Devices connect to a wide variety of networks and endpoints, making transmission of viruses faster and more deadly
- Mobile devices like cell phones are often "always on" in terms of WiFi and Bluetooth, giving hackers ample opportunity to gain access
- People like to use their personal devices at work, but they don't like to have work applications and controls installed onto their personal devices

Resisting the bring-your-own-device (BYOD) movement is not the best solution. If personal devices are disallowed, employees may invent workarounds that introduce security risks that are more serious than the ones avoided in the first place. The best approach is to design a secure way that employees can use their own equipment to do their work without increasing risk to the organization. Offer employees the ability to do the right thing from the start by developing an enterprise app store for approved apps, offering secure social media for corporate use and providing a safe "sandbox" for employees to use unapproved apps safely.[11] Remember that by allowing employees to use their own devices, an organization can save money by not having to buy new devices every few years. By reinvesting some of that savings into the alternatives above, an organization can engineer a win-win scenario for all.

Portable Media

Portable media are a prime target for cybercriminals interested in identity theft, insurance fraud, and financial theft. Portable media include thumb drives, CDs and DVDs, backup tapes, x-ray films, and other types of storage that an organization may use to transport or archive data. Loss and theft of portable media have affected more individuals than any other type of breach.

In addition to setting and enforcing clear policies and procedures surrounding the use of portable media, it is also important to employ technical safeguards. The best way to secure personal health information (PHI) on portable media is through encryption. Portable media that contain PHI should always be encrypted and password-protected. In the U.K., encryption of CDs in a medical environment is required by law. (Unfortunately, a rise in competing proprietary encryption methods among vendors there has hindered data sharing between hospitals.)

Advanced organizations can increase security by looking for ways to reduce the use of portable media altogether. For instance, consider transferring images via a cloud service, rather than burning CDs and handing them to patients.[12] Or, use a secure online backup service rather than relying on employees to transport discs and tapes physically to offsite locations, where they may get stolen out of a car.

Portable media leaving the facility can be a source of data breach, but beware, too, of *incoming* portable media. It is common practice now, for instance, for providers to give patients parts of their record or copies of diagnostic images on CDs for the patient to pass along to the next physician. The risk of accepting a CD from an unknown source is not insignificant, though. Cybercriminals can load malware onto a disc and potentially gain access to the receiving organization's network if the proper safeguards are not taken to accept only approved content types and to run only approved executable files.

Medical Devices

Medical devices are a new target of choice for cybercriminals out to wreak havoc by causing equipment failures and malfunctions. Targeted medical devices include IV pumps, blood gas analyzers, pacemakers, compounders, radiology equipment and nuclear-medical delivery systems. Increasingly, hospitals are finding that medical devices are susceptible to software viruses and malware. As was described at a recent conference of government security experts, these infections can clog patient-monitoring equipment and other systems, rendering the devices unusable and presenting a substantial patient safety risk.[13]

To date, no medical injuries have been reported in the United States as a result of infected medical devices, but sophisticated viruses have been "running rampant" according to some officials and hospital IT staff. One recent survey of 56 CIOs found that 36% had had one or more medical device malware infections in the past 12 months, with 13% reporting multiple instances and 17% attesting to an increase in occurrences during that period.[14]

Much of the problem lies with the use of outdated operating systems that have not been updated after the initial installation. In the interest of safety (and perhaps to minimize their own development costs), medical device manufacturers typically refuse to allow the routine updates and patches from operating system vendors that are intended to address security or performance issues. Healthcare organizations have also tended to avoid "tinkering" with medical device software in order to extend the life of the device and to minimize the risk of invalidating warranties, compromising functionality or violating FDA regulations. Achieving comfort and confidence in this area will take time.

Provider organizations should ensure that devices are virus-free prior to installation.[15] They should also work conscientiously with medical device vendors to lock down their devices and make them less vulnerable. In the meantime, this category of threat is a grave reminder to organizations that security is more than avoiding breach notification penalties — it's also about life and death.

Gaining Confidence

Health IT security no longer can be about locking down individual applications and systems; today's threats require a holistic approach. Achieving *cyberconfidence* means the ability to engage securely with patients, partners and others in a context of mutual trust. It is the knowledge that the organization can react to any threat or incident with speed and agility. One step along the way is to perform a comprehensive risk assessment, either internally or in concert with outside experts. Organizations interested in enlisting additional outside expertise can also consider using a managed security service.

The Comprehensive Risk Assessment

An important step toward achieving cyberconfidence is to conduct a comprehensive risk assessment. A risk assessment identifies and documents the current state of an organization's security capabilities and risk profile. It is a complete review of the security posture of an organization, mapped against accepted industry standards, regulatory requirements, and any special policies and practices needed to meet the needs of the particular organization.[16] In areas of deficiencies, an assessment would ideally also include a proposed migration plan to achieve compliance with state and/or federal law.

For healthcare providers participating in the EHR meaningful use incentive program, the risk assessment is required for attestation. To demonstrate meaningful use of EHRs, providers must perform a security risk analysis and address any weaknesses identified.[17] A key part of the assessment is the accompanying analysis and documentation of findings. Always document all decisions and changes made, including reasons for why various actions were deferred.

A comprehensive risk assessment is also required for compliance with the HIPAA Security Rule. To minimize the risk of a data breach, covered entities and their business associates must assess their risk and identify where they are most vulnerable.[18] The inclusion of business associates (BA) is important, given recent expansion of HIPAA applicability. Staff should identify the relevant contractual obligations with BAs and request documentation pertaining to BA's recent security audits.[19]

An unexpected benefit of doing a risk assessment is that it can also clarify to what you *don't* have to do. Advice on security practices and compliance is not always consistent. You may think or have been told that you need to do something in order to secure your system or become HIPAA-compliant, and you may be spending a lot of money on it. A thorough assessment might save money.

An organization can undertake its own risk assessment or enlist the help of outside experts. Publicly-available tools can help an organization go the former route if desired. For instance, the Office of the National Coordinator for Health IT (ONC) has made available a web-based security training module called

CyberSecure: Your Medical Practice. The online training module presents healthcare-specific privacy and security challenges and quizzes users about the scenarios. ONC also has a guide for physicians on evaluating security practices and a cyber-security checklist available.[20] Similarly, in June 2012, the Office of Civil Rights (OCR) released the protocol that it is using to conduct HIPAA audits. The audit program addresses a total of 165 performance criteria surrounding security processes, controls and policies. The documentation details what is expected of organizations and how they will be evaluated during an audit. OCR is advising covered entities to use the protocol to evaluate their own audit readiness.

A risk assessment should also include a review of the policies and procedures for how to handle a breach once it has occurred. Data breaches happen to even the best of organizations. Having a sound and defensible response plan that has been well thought out and rehearsed with leadership, staff, and BAs can help CIOs sleep better at night.

If it has been a long time since an organization's last review of its security practices, then performing a comprehensive risk assessment is a critical first step toward cyberconfidence. However, it is not a one-time event. Risk assessment needs to be an ongoing process of reviewing records, tracking progress, evaluating security incidents and evaluating the overall effectiveness of the security measures that are in place.[21]

The Managed Service Option

With security threats becoming ever more complicated and difficult to keep pace with, many organizations are turning to managed security service providers (MSSPs). This option enables an organization to outsource all or part of its IT environment from a security standpoint.

Information security is changing as a discipline. It is no longer a function that must remain in-house.

MSSPs provide 24-hour network monitoring, incident tracking and immediate incident response. This level of detection and response is critical to an organization's security. A recent review of healthcare data braches found that nearly two-thirds of the breaches persisted for months before they were detected, giving criminals ample time to do damage. In many of these cases, the organizations were unaware of the breach until they were notified by law enforcement officials or credit card companies. Clearly healthcare organizations are not as capable of detection and response as they may believe.

Because managed security service providers deal with the security challenges of many companies across many industries, they have a broader and deeper view of security issues. They've addressed more security vulnerabilities than most healthcare organizations will ever encounter.

Analysts estimate growth in the managed security space at 30 to 40% per year.[22] This is due mainly to increased confidence among CIOs in MSSPs to offer key advice and strategic value. MSSPs offer not just the opportunity for cost savings but also access to sophisticated security tools and top talent. Interest will continue to grow as MSSPs further mature into trusted partners.

Going the managed security route can be easier and more affordable than the do-it-yourself route, since all an organization needs to do is select the services they need, and pay for only the services and resources that they consume. A managed security service has the expertise and ability to handle the minutiae of patches and fixes as soon as they are discovered. Small issues do not build up over time like they can in a traditional environment. For many organizations, less than 10% of their annual IT budget is allocated to data security, placing significant strain on those whose job is to protect some of the organization's most valuable assets. In a recent survey of healthcare IT executives, three-fourths of respondents said that the organizations lacked sufficient funding to prevent such breaches.[23] For organizations facing these types of constraints, managed security may be the best (if not the only) way to achieve a high level of cyberconfidence.

Case Study: Assessment and Remediation at a Large Health System

A large nonprofit health system in the western part of the United States decided to undergo a voluntary audit of its privacy and security practices in preparation for an official government audit that the organization is anticipating in 2013. This health system serves over twenty hospitals in two states. It is consistently ranked highly in IT practices, and spoken of favorably on the national stage.

Like many organizations, this health system is facing increasingly sophisticated attacks from cybercriminals, and increased compliance pressures from federal and state regulations. The organization had not had any high-profile breaches, but it knew that its security practices needed to be reviewed and evaluated. For instance, many of its security procedures were communicated verbally and were not captured formally. In order to ensure that it protects patient information and maintains the public trust, it conducted an initial risk assessment internally and turned to outside security experts for additional evaluation and remediation.

The collaborative effort focused on five areas agreed upon as important to maintaining an effective enterprise security posture:

1. **Security Audit Readiness**. Identified the information and documentation that would be needed to respond to an audit by/for OCR, HIPAA, HITECH or any other reason.

2. **Security Policies and Procedures**. Reviewed and ensured that policies and procedures were up to date and aligned with current statutory and regulatory requirements, as well as industry standards and best practices.

3. **Security Awareness, Education and Training**. Evaluated and updated the organization's security awareness training to be in line with best practices. Evaluated the differences in training given to staff members in different roles and ensured that they were appropriate.

4. **Security of Applications, Data and Networks**. Identified all applications and their associated data (at rest and in transit), so that appropriate security measures could be taken to protect and secure such data and applications. Segmentation and secure enclaving of data storage were used to provide additional security.

5. **Encryption of Data**. Developed a strategy to encrypt high-value enterprise data and systems containing ePHI, and coordinated this with a broader data protection strategy protecting data both at rest and in transit. Encryption and other protection spanned the full gamut of storage area networks, devices, databases, applications and more.

Throughout the effort, the organization and the security experts utilized standards such as the HITRUST Common Security Framework, HHS Security and Privacy guidance documentation, ISO standards, and standards from NIST standards where appropriate.

The health system's environment has now been updated and is able to protect against modern threats. In working with a trusted security partner, they were able to have a successful assessment and remediation effort that incorporated innovative technologies, and that elevated the discussion to a more strategic level than before.

Recommendations: 5 Next-Generation Ideas for Your Next Security Meeting

Healthcare organizations concerned about security need to start with a comprehensive risk analysis, so that they understand what the threats are, what their vulnerabilities are, and what gaps there are between their current practices and accepted industry standards. To gain full confidence, however, organizations also need to make security part of an ongoing process of improvement. They need to move beyond a narrow view of security and toward an approach that ties together security, compliance, risk management and corporate governance. For some organizations, managed security is the smartest route.

Regardless of where your current organizational risk profile stands, here are five next-generation ideas and recommendations that are worth considering at your next high-level security meeting:

Five Next-Generation Ideas to Consider

1. Deploy advanced network monitoring.
2. Develop a 21st century strategy for mobile devices and medical devices.
3. Make system authentication multi-factor and adaptive.
4. Test yourself by contracting with ethical hackers.
5. Consider whether purchasing cyber insurance might be right for you.

1. **Deploy advanced network monitoring**. Organizations need automated tools to assess vulnerabilities and be on the lookout for breaches. Seek out advanced tools to self-test the effectiveness of your firewall. Consider egress solutions, which automatically monitor what is being sent outside the walls of an organization, where it is being sent and when. Allow outgoing channels to be locked down automatically if special conditions are met. If you don’t have these capabilities, consider going the managed security route with a trusted managed security service provider.
2. **Develop a 21st century strategy for mobile devices and medical devices**. You cannot fight the bring-your-own-device movement, but you *can* manage it and help employees make good decisions. Embrace security practices that are easy for end users. Nurses have little patience for application latency and will share passwords if user profile restrictions are too burdensome. Similarly, doctors have very little patience for being asked to remember multiple passwords and user names. Find a balance that is amenable to security without disrupting workflow. As for medical devices, hospitals cannot afford to be ignorant of the presence of viruses and malware on medical devices. To address these concerns, try integrating part of the IT security function with the biomedical engineering services department. Build a culture and processes that foster communication between these groups on the topic of security. Encourage the sharing of security intelligence, surveillance and problem reports.
3. **Make system authentication multi-factor and adaptive**. Multi-factor authentication systems are much preferred over systems that use just passwords. Multi-factor systems are expensive and take a long time to deploy, so get a head start before they become required by HIPAA, which is conceivable within the next few years. On the market today are biometric patient identification systems based on fingerprints, palm vein patterns and more that help guard against medical identity theft and insurance card fraud, and ensure that IT systems are safe. User authentication requirements should also change dynamically based on risky behavior. Adaptive systems challenge people more or less based on where users are logging in from, what they are trying to access and what they have attempted to access already.

4. **Test yourself by contracting with ethical hackers**. The idea of using ethical hackers — employing people with hacker-like skills to try to find exploits from the outside — has received a lot of press. It is no substitute for conducting a risk assessment or using a managed security service, but it can help to identify more obscure vulnerabilities that may have been overlooked. Ask ethical hackers to test your technical environment, as well as the training of your staff (i.e., through social engineering). This can become a training exercise for employees.
5. **Consider whether purchasing cyber insurance might be right for you**. New insurance products on the market are designed specifically with hospitals and other healthcare organizations in mind. One prominent insurer provides coverage that helps defray costs related to data breaches, including legal defense, privacy notification expenses, and certain regulatory fines and penalties. While insurance won't make your systems any more secure, it can help you feel more confident about your ability to survive a major adverse incident.

Keeping up with cyber threats can be challenging, but IT security should not hinder an organization's growth or prevent it from using data assets to improve care delivery, quality and financial performance. With increased vigilance and the right technological tools, it is possible for healthcare organizations to achieve true confidence in their cybersecurity.

Acknowledgments

The author would like to thank Ashif Jiwani, CSC Partner, and Jordan Battani, Managing Director of the Global Institute for Emerging Healthcare Practices, for their contributions to this paper.

About the Authors

Jared Rhoads is a senior research specialist with CSC's Global Institute for Emerging Healthcare Practices, the applied research arm of CSC's Healthcare Group. Richard Staynings is Cyber Security and Privacy Officer for CSC.

References

1. “2012 Data Breach Investigations Report.” Verizon Communications, October 2012.
2. “American Hospital Association Exclusively Endorses Chubb’s Cyber Insurance Product for Health Care Organizations.” Chubb Group, October 1, 2012.
3. “Healthcare Fraud Medical Identity Theft Inaccurate Patient Identification” M2Sys, October 2012.
4. “CSC Cybersecurity: Delivering Cyberconfidence” CSC, Accessed October 10, 2012.
5. “2012 Data Breach Investigations Report.”
6. “A glimpse inside the $234 billion world of medical fraud.” Government Health IT, February 8, 2012.
7. Bailey, D. “Identity Theft Check Up: Electronic Medical Records Are the New Credit Cards.” Redspin, March 3, 2010.
8. “Cybersecurity is a big concern for medical organizations.” *Geeks On Site*, Accessed October 10, 2012.
9. “HITECH Act Three Years Later: Are Health Records Safe?” Kaufman Rossin Co., July 24, 2012.
10. “The Security Landscape: Converging Waves of Pain.” CSC, Accessed October 10, 2012.
11. Patterson, T. “How a Recent Study Got It Wrong: Lower Budgets not Reducing IT Security.” CSC, October 4, 2012.
12. “HITECH Act Three Years Later: Are Health Records Safe?”
13. “Computer Viruses are ‘Rampant’ on Medical Devices in Hospitals.” *Technology Review*, October 17, 2012.
14. Ochoa, G. “Homeland Security Warns About Medical Device Threats.” *Anesthesiology News*, October 2012.
15. Ibid.
16. “Enterprise Security Roadmap for Healthcare.” CSC, Accessed October 9, 2012.
17. Mosquera, M. “ONC offers online security training game.” *Government Health IT*, September 12, 2012.
18. “HITECH Act Three Years Later: Are Health Records Safe?”
19. “Enterprise Security Roadmap for Healthcare.”
20. Mosquera.
21. “HITECH Act Three Years Later: Are Health Records Safe?”
22. Ferrara, E. “The Forrester Wave: Managed Security Services: North America, Q1, 2012” Forrester Research, March 26, 2012.
23. “Cost of Data Breach Study.” Ponemon Institute, February 2012.

Healthcare Group
3170 Fairview Park Drive
Falls Church, VA 22042
+1.800.345.7672
healthcaresector@csc.com

Worldwide CSC Headquarters

The Americas
3170 Fairview Park Drive
Falls Church, VA 22042
United States
+1.703.876.1000

Europe, Middle East, Africa
Royal Pavilion
Wellesley Road
Aldershot, Hampshire GU11 1PZ
United Kingdom
+44(0)1252.534000

Australia
26 Talavera Road
Macquarie Park, NSW 2113
Australia
+61(0)29034.3000

Asia
20 Anson Road #11-01
Twenty Anson
Singapore 079912
Republic of Singapore
+65.6221.9095

About CSC

The mission of CSC is to be a global leader in providing technology-enabled business solutions and services.

With the broadest range of capabilities, CSC offers clients the solutions they need to manage complexity, focus on core businesses, collaborate with partners and clients, and improve operations.

CSC makes a special point of understanding its clients and provides experts with real-world experience to work with them. CSC is vendor-independent, delivering solutions that best meet each client's unique requirements.

For more than 50 years, clients in industries and governments worldwide have trusted CSC with their business process and information systems outsourcing, systems integration and consulting needs.

The company trades on the New York Stock Exchange under the symbol "CSC."

www.csc.com

WA12_0271 HCG
November 2012