A PRACTICAL THREE-STEP PLAN TO MAKE HEALTHCARE CYBERSECURITY STRONGER

Why wait for disaster to strike? Here are three actions you can take to minimize risks and costs and recover more quickly when an attack happens.

INTRODUCTION

Healthcare accounts for 21% of all cybersecurity breaches, making it the most affected business sector in the U.S. economy.[1] Ongoing attacks are predicted to cost providers $305 billion in lifetime revenue over the next few years.[2]

Some of these attacks will resemble the one that recently hit the 24-clinic network of a U.S. company. Ukraine gangsters with a confused political agenda used a SQL injection and ransomware (a type of malicious software that encrypts data) to steal a treasure trove of sensitive data, including financial documents and patient records.[3]

It is unclear from published reports whether the clinic owner responded to the group's extortion and threats. What we do know is that the protected health information (PHI) was eventually posted online for anyone to access. The clinics now face legal liability and investigation by the U.S. Department of Health and Human Services (HHS). Because of the breach, it will have to spend significant sums to notify affected parties, conduct a thorough forensic analysis, and engage legal representation. Civil and criminal penalties may follow, depending on HHS' findings.

Also, research suggests the breach will create long-term financial consequences for the clinic if, as typically happens, almost half of its patients decide to switch healthcare providers because their medical records were not protected.[4]

CONTENTS

WHY HACKERS LOVE TO TARGET HEALTHCARE

Healthcare cyberattacks are common, according to the Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data. The study found that nearly 90 percent of providers have had at least one recent breach—at an average cost of $2.2 million.[5]

Hackers go where the data is, and healthcare has lots of data. Hackers also know that healthcare providers often deploy lower levels of security compared to sectors such as financial services and critical infrastructure, says Michael Born, vice president for the cyber and technology practice at Lockton Companies, the world's largest privately owned insurance brokerage firm.

So why isn't security better in healthcare? A reluctance to spend scarce dollars on a non-core function is part of the problem, according to the 2015 HIMSS Cybersecurity Survey.[6] But Born also thinks too many decision makers are pursuing the security unicorn. "Some organizations are waiting to deploy the perfect security system," he says. "But the reality is you can never have a perfect system for an evolving threat. If you wait until it is perfect, you will never get there."

Healthcare providers who do not want to wait for the next breach can take three important steps to improve their security posture, says Andrew Wild, chief information security officer at QTS Realty Trust. "First, providers need to proactively identify risks," he says. "Second, because even the most secure organization can be breached, they need a strategy for effectively managing the liability and costs of inevitable security breaches. Third, they need to make investments in IT and security that are in line with identified risks or consider outsourcing to a qualified third-party provider to ensure an adequate security posture."

STEP 1. PROACTIVELY IDENTIFY RISKS

When healthcare providers talk about security, they focus on PHI, which is understandable since the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule requires providers to protect individually identifiable health information.[7] The more recent HIPAA Security Rules add additional cybersecurity compliance requirements for PHI through administrative, technical, and physical safeguards.[8] Subtitle D of the Health Information Technology for Economic and Clinical Health (HITECH) Act applies as well.[9] Violations of these acts are investigated by the HHS' Office of Civil Rights (OCS) and subject to civil penalties and criminal prosecution by the U.S. Department of Justice. The Federal Trade Commission (FTC) is also taking an aggressive stance on cybersecurity. Recent actions, such as the FTC's audit of Atlanta-based LabMD, suggest that companies can be subject to enforcement actions even when there is no evidence of a breach or injury caused by unauthorized data disclosures.[10]

Meeting these mandates is impossible unless an organization understands its vulnerabilities. These exposures include not just data stores but also computer systems and medical devices that can be controlled, damaged, and/or rendered inoperable by an attack. The best way to identify areas of exposure is by undergoing a cybersecurity risk assessment. The National Institute of Standards and Technology (NIST), a federal agency, notes that the goal of an assessment is to understand the risks associated with an organization's operations, assets, and individuals.

WHAT A CYBERSECURITY ASSESSMENT ENTAILS

Most healthcare providers are not staffed or equipped to conduct an investigation. An at-risk organization needs to hire a cybersecurity firm with a deep understanding of the healthcare industry, its technology environments, and the inherent risks associated with its workforce and systems.

A good consultant will base its assessment strategy on an established framework, such as the NIST Cybersecurity Framework, the Center for Internet Security Critical Security Controls, the ISO/IEC Information Security Management Systems standards (ISO 27000), the Control Objectives for Information and Related Technologies framework, the Health Information Trust Common Security Framework, or a custom cybersecurity framework tailored to an industry's unique vulnerabilities. Any of these approaches provide a common set of ground rules for:

+ Describing a healthcare provider's current cybersecurity posture and target state
+ Identifying and prioritizing opportunities for improvement within the context of a continuous and repeatable process
+ Assessing progress toward the target state
+ Communicating among internal and external stakeholders about cybersecurity risk[11]

The assessment itself should replicate the tactics, techniques, and procedures (TTPs) that hackers are likely to use to breach a provider's defenses. If the tests are not appropriate or realistic, the countermeasures suggested by the consultant may not provide effective improvements for the organization's security.

WHAT TO DO AFTER THE ASSESSMENT

An effective cybersecurity assessment will provide a roadmap for meeting minimum requirements along with additional steps for further reducing data vulnerability. NIST suggests the assessment report should:

+ Provide a prioritized, flexible, repeatable, performance-based, and cost-effective approach
+ Help infrastructure managers identify, assess, and mitigate cyber risk
+ Enable technical innovation while accounting for organizational differences
+ Include guidance for measuring the performance of recommended changes

While many issues are subject to security mandates, policies often allow organizations to implement the more cost-effective response. It is important to consider if the cost-effective response is adequate to address the rapidly evolving threat landscape. A knowledgeable cybersecurity specialist can help an organization weigh the risks of minimum compliance as well as the costs and benefits of stronger security measures.

Invariably, improving security also requires a healthcare provider to overhaul deeply embedded practices and worker behaviors, such as clicking on email attachments, leaving computers and terminals unsecured in patient exam rooms, and accessing sensitive data with personal devices (what some call the bring-your-own-device phenomenon). Changing or controlling these practices and behaviors is a difficult but essential part of the process, says Wild. "Compliance is the first step towards a mature, adaptable security posture," he says. "Implementing best practices in cyberspace and the real world is a great start, but mature security programs require a culture change to be successful. Security has to become part of how all employees – from surgeons to administrators – do their jobs. It cannot be simply an IT responsibility."

STEP 2. TRANSFER RISKS AND MORE EFFECTIVELY MANAGE COSTS

Remediating vulnerabilities improves cybersecurity, but even the best vulnerability management programs cannot remediate 100 percent of all vulnerabilities, so companies also need to consider cyber insurance, which can transfer some of the risk of a security breach. Currently, 59 percent of private and public-sector companies have purchased policies or are planning to purchase policies within the next 24 months.[12] Basic policies cover claims resulting from data privacy and data security breaches, which are two distinct categories of coverage.

Bill Boeck, senior vice president, insurance and claims counsel at Lockton Companies LLC, notes in the Lockton Cyber Risk Update Blog that data privacy claims concern the improper disclosure or exposure of private information, which includes personal, credit card, health, and confidential business information. Claims generally are brought by individuals and companies whose private information has been compromised or by regulators or law enforcement. Data security claims involve losses arising from beaches of the insured's computer systems, which usually is the result of a hack or a distributed denial of service (DDoS) attack that affects the delivery of healthcare services.

WHAT TO LOOK FOR IN A CYBER INSURANCE POLICY

Cyber insurance is offered by a number of companies. Comprehensive policies are complex and designed to offset the expenses related to:

+ Cyber extortion
+ Cyber event investigation
+ Customer notification
+ Credit-monitoring services for affected parties
+ Good-faith advertising to repair marketplace reputation
+ HIPAA fines
+ Cyber attacks on computer systems
+ Defense costs and damages from privacy related claims or lawsuits

When a healthcare provider evaluates cyber policies, it should look for coverage that includes liability to third parties and regulators for privacy breaches, liability to third parties for computer breaches, and first-party liability to recover breach-related forensic and response costs. Engaging an insurance broker with specialized expertise in cyber exposures and insurance solutions can provide invaluable assistance while navigating this new and complex type of insurance coverage.

HOW A CYBER INSURANCE EXPERT HELPS DEFINE THE BEST COVERAGE AT THE LOWEST PRICE

Insurance is about shifting liability to an insurance provider, and cyber insurance is no different. At the same time, the unique liability risks associated with cyber breaches and PHI make underwriting this type of coverage complicated. Working with an insurance broker that has technology and industry expertise is critical to ensuring that coverage and policy limits are adequate for the owner's level of risk.

"Coverage amounts will be different for each type of policy," Boeck says. "Companies need to consider sublimits carefully. I have seen a number of claims over the years where companies wished their sublimits had been higher."

An experienced agent, broker, or attorney also can advise a healthcare provider after a breach and help to minimize mistakes that might increase fines or other costs.

"Legal liability for data and network security breaches is still evolving with disparate or outright conflicting decisions among the courts that have addressed these issues," Born says. "Companies need to work with a specialist in the cyber liability field that understands the shifting legal landscape."

Legal liability is also influenced by statements from regulators, such as Luis A. Aguilar, who as head of the Security and Exchange Commission, advised companies that their boards of directors should include members with expertise in cyber risk.[13] "Given the significant cyber-attacks that are occurring with disturbing frequency, and the mounting evidence that companies of all shapes and sizes are increasingly under a constant threat of potentially disastrous cyber-attacks, ensuring the adequacy of a company's cybersecurity measures needs to be a critical part of a board of director's risk oversight responsibilities," he says.

Many organizations find that their security posture improves with the purchase of cyber insurance. Before an insurer will issue a policy, the application process typically requires applicants to undergo a security assessment and implement the sort of security upgrades we discussed earlier.

STEP 3. MOVE DATA AND PROCESSING TO A QUALIFIED AND TRUSTED CLOUD PROVIDER

While absolute cybersecurity is impossible, healthcare providers can reduce their exposure by addressing risk and investing in insurance. But progress takes more time than many decision makers fully appreciate, says FBI supervisory special agent Scott Augenbaum.[14] "It takes a full three to five years to implement a comprehensive IT security strategy," he says. "People simply don't understand this."

What healthcare providers do seem to understand is that they are falling short on security. Nearly 60 percent of providers believe their security spending is not sufficient to limit breaches.[15] Staffing also is an issue, with the industry reporting more than 20,000 open positions in healthcare IT security.[16] The staffing issue is not likely to be resolved any time soon given the global shortage of trained information security professionals.

At the same time, up to 50 percent of healthcare providers are holding IT security spending at current levels while an additional 10 percent are actually cutting spending.[17] In response to inadequate budgets and a dearth of technical talent, some decision makers are considering following other industry sectors to the cloud, where scale and specialization may give them an affordable way to be technologically capable and secure.

WHY THE CLOUD IS GAINING GROUND WITH HEALTHCARE

In 2015, the healthcare cloud computing market in the U.S. was worth about $2.3 billion dollars but is expected to grow significantly to $5.8 billion by 2020.[18] Eventually, up to 80 percent of healthcare data potentially could pass through the cloud.[19] However, both trends may accelerate if healthcare providers experience more breaches and stronger regulatory pressure to mitigate risk.

A cloud service provider (CSP) offers resources to organizations that need to store, manage, process, and protect data. Because it specializes in providing compute resources and environments, it is able to offer more advanced, secure, scalable, and resilient infrastructure and technical services for less cost than an organization can typically create on its own.

A healthcare provider can choose service and deployment models that improve its IT capabilities while potentially reducing long-term costs. While outsourcing to a CSP does not negate the need for security measures or cyber insurance, it enables a provider to transfer the cyber-protection task to an organization that views IT as its core mission.

A CSP that offers services to the healthcare market is considered a business associate under HIPAA.[20] As a business associate, it must conform to the same laws, rules, and regulations that govern other healthcare-related organizations. The HSS Office for Civil Rights (OCR) is responsible for auditing CSPs and determining if they meet HSS' technical safeguard for creating, receiving, maintaining, and transmitting PHI.

WHAT TO LOOK FOR IN A CLOUD PROVIDER

A healthcare provider should select a CSP that operates its own HIPAA and HITECH compliant data center. Some CSPs offer compute resources, but they rely on third parties for data storage and physical and environmental controls. A fully integrated CSP has complete control of its cloud and is better positioned to protect a provider's PHI data while also providing high-performance infrastructure for expanding access and portability. A careful evaluation of a CSP is critical since moving data to the cloud does not absolve a healthcare provider of liability should its data stores suffer a breach.

"It is important to remember that you cannot contract around the law," says Shirley Goza, general counsel at QTS Realty Trust. "The healthcare provider is still responsible for the PHI."

A candidate CSP should demonstrate rigorous compliance with all applicable laws and regulations. And it must provide Business Associate Agreements (BAA) describing how much of the compliance burden and associated liability it will be assuming. A CSP that cannot provide a BAA probably lacks the technology, staffing, and practices to ensure compliance with legal mandates and industry best practices.

On the technical side of its operation, the CSP's infrastructure must offer sufficient scale to meet not just current needs, but also any requirements that the healthcare provider believes may emerge over the long-term. Similarly, the CSP should provide outstanding physical security for all its facilities, 24/7 support, and self-service management over the web or through an application program interface. For healthcare providers that want to streamline internal overhead, the CSP's staff should include a deep bench of IT experts who can help to reduce security and compliance risks, control costs, and improve operational efficiencies.

HOW TO ACT AND MITIGATE RISK

Healthcare providers are vulnerable to cyber attacks, but they can take steps to reduce risk and mitigate the consequences of data breaches when they occur. Waiting for the market to deliver the perfect security system is unwise because such a solution will never exist. Improving cybersecurity is an ongoing process that involves proactively identifying and addressing risks, effectively managing the costs of an inevitable security breach, and investing in IT or outsourcing key IT functions to a qualified third-party provider. The most dangerous thing healthcare providers can do in the current environment is to maintain their status-quo approach to security.

RESOURCES

[1] NetDiligence 2015 Cyber Claims Study, 2015, p. 3.

[2] The $300 Billion Attack: The Revenue Risk and Human Impact of Healthcare Provider Cybersecurity Inaction, Accenture, 2015.

[3] Central Ohio Urology Group hacked, PHI dumped: hacktivist (Updated), www.databreaches.net, August 2, 2016.

[4] Ibid. Accenture.

[5] Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data, Property Casualty Insurer Association of America, May 2016, p. 1.

[6] 2015 HIMSS Cybersecurity Survey Executive Summary, Health Information and Management Systems Society, June 30, 2015.

[7] The HIPAA Privacy Rule, Department of Health and Human Services, August 2016.

[8] Summary of the HIPAA Security Rule, Department of Health and Human Services, August 2016.

[9] HITECH Act Enforcement Interim Final Rule, Department of Health and Human Services, August 2016.

[10] FTC Reasserts Data Security Authority in LabMD Ruling, Bloomberg Law, Jimmy H. Koo, August 1, 2016.

[11] Framework for Improving Critical Infrastructure Cybersecurity, National Institute of Standards and Technology, February 12, 2014.

[12] Cyber Catastrophes: Understanding the Risk and Exposure, Property Casualty Insurer Association of America, March 2014, p. 5.

[13] Boards of Directors, Corporate Governance and Cyber-Risks: Sharpening the Focus. Commissioner Luis A. Aguilar, Cyber Risks and the Boardroom Conference, June 10 2014.

[14] Healthcare Leaders Need to Move Faster to Meet Cybersecurity Challenges, CHIME/AEHIS Lead Forum Event Address, August 19, 2016.

[15] Ibid. Property Casualty Insurer Association of America, p. 2.

[16] Ibid. Property Casualty Insurer Association of America, p. 4.

[17] Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data, Property Casualty Insurer Association of America, May 2016, p. 4.

[18] Healthcare Cloud Computing Market press release, MarketsandMarkets, June 2015.

[19] IDC FutureScape: Worldwide Healthcare 2015 Predictions, IDC, November 12, 2014.

[20] Final HIPAA Omnibus Rule: How It Changes Cloud Computing for Healthcare, Online Tech.

CONTRIBUTORS