Addressing the Growing Threat of Cybersecurity in Healthcare

Produced in partnership with

Xtelligent Media

Understanding the Current State of Healthcare Cybersecurity

Healthcare cybersecurity is an increasingly important issue for both covered entities and business associates, especially as the online threats continue to evolve.

Healthcare organizations need to understand the existing threats so they can create comprehensive data security strategies that will work to mitigate those issues. The targeted cyberattacks are increasing in healthcare, and entities need to know what types of attacks they could eventually face.

Whether it's a phishing attack, ransomware attack, or an unauthorized third-party hacking into a network, healthcare cybersecurity has evolved into an issue that is no longer just relegated as an "IT problem."

Regulatory changes have been put into effect recently, but that does not mean that covered entities can assume that they will be protected. Employee training and regular reviews of the entire data security approach are also essential aspects to keeping sensitive data secure. Moreover, the C-suite must also take heed to the increasing threats, and take the necessary steps to help create the right approach to threat protection, detection, and reaction.

What are the current regulations on cybersecurity?

The Cybersecurity Act of 2015 is a crucial piece of legislation that was passed toward the end of 2015. The goal was to create a framework for exchanging information regarding cybersecurity threats within the numerous industries, such as healthcare.

Additionally, industry professionals would be able to connect via a network so that they can better exchange information with one another regarding potential cybersecurity threats.

The White House has also been making moves to ensure better cybersecurity across the nation, in the healthcare industry and others. In February, President Barack Obama announced the implementation of the Cybersecurity National Action Plan (CNAP).

It is important "to enhance cybersecurity awareness and protections, protect privacy, maintain public safety as well as economic and national security," the White House explained.

The Commission on Enhancing National Cybersecurity was also launched, which will be supported by the National Institute of Standards and Technology (NIST). The Commission will make "detailed recommendations on actions that can be taken over the next decade to enhance cybersecurity awareness and protections throughout the private sector and at all levels of Government."

In terms of healthcare cybersecurity specifically, the Office for Civil Rights created a crosswalk to help organizations understand the connections between HIPAA regulations and the NIST Cybersecurity Framework (CSF).

It is important for covered entities to identify "mappings" between the two frameworks, according to OCR, and it is important to watch for potential gaps. A facility may have implemented one or both approaches to security, but something may have been overlooked. The crosswalk hopes to highlight those gaps and suggests how organizations can better align their security in a digital age.

"Although the Security Rule does not require use of the NIST Cybersecurity Framework, and use of the Framework does not guarantee HIPAA compliance, the crosswalk provides an informative tool for entities to use to help them more comprehensively manage security risks in their environments," OCR explained in the crosswalk.

What are the current types of cyberattacks?

With more healthcare organizations using connected medical devices, implementing BYOD strategies, and working toward interoperability, covered entities have more potential exposure points than ever before.

Not only can unauthorized users hack into a network, cyberattacks could also come in the form of phishing attacks or a ransomware attack.

A phishing attack is typically a type of email or social engineering attack, where cyber attackers attempt to trick individuals into releasing personal information. This could be an email to a CEO or to a nurse or physician. Individuals could also be directed to a website where they are directed to enter in personal information.

Healthcare phishing and vishing scams are usually trying to access sensitive patient information from employees, or company information that can then be used to gather patient data, or to entice them to click on a link or open an object that could result in a connection to a rogue server, and the introduction of malware onto the user's system, such as Ransomware.

For example, if an employee believes a phishing email to be legitimate, he or she may unknowingly give their username or password to an unauthorized third party. This can also occur over the phone, if a user is coerced into giving sensitive information to a caller they believe to be authorized (vishing). From there, the cyber attacker might be able to log on to a provider's system and gain access to PHI or other sensitive company data.

Ransomware is also becoming an increasingly popular method of attack against healthcare organizations. This is a type of malware that will prevent an organization from accessing certain parts of its system. Essentially, a company's information is held hostage.

There are two basic types of ransomware: crypto ransomware and locker ransomware. The former will encrypt data, with employees potentially unable to read patient information, while the latter prevents users from accessing the data entirely.

"Ransomware is less about technological sophistication and more about exploitation of the human element," explains the Institute for Critical Infrastructure Technology (ICIT) in its recent ransomware report. "Simply, it is a digital spin on a centuries old criminal tactic."

Ransomware could potentially be downloaded through a phishing scam, so employees must be properly trained on what suspicious emails could potentially look like, and what to do if one is found.

Mitigation tactics are essential, but it is important to remember there is not a silver bullet to ensure that a cyberattack never occurs. Software and hardware solutions must be regularly updated, and organizations should implement tools such as antivirus, firewalls, and consider data encryption., as well as ensure the proper policies and procedures are in place, and that the workforce (people) are trained to enforce them.

Addressing the Business Challenges of Healthcare Cybersecurity

Understanding the business challenges of implementing a new technological solution is an important first step for healthcare organizations.

Whether an organization is looking into cloud storage, mobile device options, or another technical tool, keeping data security a top priority is essential.

Having full comprehension of any business challenges is important because that way, when any type of an architectural solution is prepared, the organization is meeting whatever the business process requirements are of that particular customer or environment, says PC Connection Practice Director of Security and Mobility Stephen Nardone.

"Certainly in a healthcare space that's extremely important," he explained. "For example, is mobility a challenge and something that they're interested in to enhance the efficiency of their clinical process? If so, understanding the business requirments, and documenting the policies and controls necessary to meet those challenges in a safe and secure way is crucial. Understanding that whole business process is really key."

Conducting an analysis of where the organization stands from an overall risk management perspective is the next step. Covered entities should ask what types of process they have put in place, as well as what tools or techniques are being associated with the assessment. The testing that is required to better understand risk is also a key aspect to this.

"What does the organizational structure look like in the healthcare environment? Do they have the appropriate IT staff, security staff, organizational structure, etc., across the entire environment?" asked Nardone. "That's the information that I like to make sure I understand before I even take that first step of trying to advise any type of a healthcare customer what they really should be thinking about from a security risk management perspective."

Understand security requirements for better protection

A broad mistake that Nardone sees healthcare organizations make is not fully understanding security requirements. Whether it's the HIPAA Security Rule that a facility's staff members do not understand, or just employees not knowing what the organization's privacy policy is, he explains that this is an area that cannot be overlooked.

"Because HIPAA is not necessarily a process that has a strict governance oversight associated with it, a lot of healthcare entities think, 'It's not going happen to me,'" so I can ignore doing an annual HIPAA Security Audit, Nardone maintained. "Every healthcare institution needs to make sure that they are reviewing their overall security capability to meet the HIPAA standards, the HITECH standards, or the HITRUST standards. Whatever it is they need to achieve in order to be able to make sure that they've done the appropriate level of audit and compliancy."

Another key oversight is that healthcare organizations might not have a proper understanding as to what their business process really needs to be.

"For example, clinicians may need to have portable devices in order to be able to handle the ability to deliver the quality healthcare they need to at the bedside or in a structured clinic environment," Nardone explained. "If that's something that is important as a business requirement, there are a whole set of infrastructure and security requirements that need to be determined and implemented in order to be able to make that happens in a safe and secure way."

Lessons learned from 2015 healthcare data breaches

There is no question that the healthcare industry is a target when it comes to data breaches, Nardone said. Whether the issue is medical identity theft or breached electronic medical records, the large-scale data breaches that took place last year hold important lessons for stakeholders.

"It's very clear that healthcare is a target," he reiterated. "This is not just coincidence that these environments are being breached. They are a target, and anybody that's in a security-related position supporting a hospital or a covered entity really needs to make sure they're paying attention to that threat. It's not if it might happen. It is going to happen, and they need to make sure that they're paying attention to that threat."

Looking ahead to 2016, Nardone maintained that every covered entity must put in a process to best determine its potential risk factor.

"They need to be putting in place a process whereby they are constantly testing and validating their ability to be able to manage against that risk," he voiced. "Organizations also need to put a strategy together that includes an information security program and an information security risk governance program."

Those programs must be adopted all the way through to the highest levels of the institution and also supported by the C-level suite, Nardone added. It is also important that there is a plan for how those covered entities are going to constantly monitor and manage that risk over a period of time.

There is no silver bullet in the security industry, Nardone concluded.

"It really requires a well-balanced, structured security ecosystem in your environment with the appropriate level of technology, process, and people to help manage security risk," he explained. "It's about covering your complete end-to-end infrastructure, from endpoint to data security to securing all your critical applications in your data center, to tight access controls and monitoring for network protection."

If the overall information program and risk governance strategy is being done well, it is supported by some form of 24/7/365 managed security services. Whether it's through internal resources or from an external provider, the constant program and system monitoring is important.

"All of those things are crucial to really getting this right."

How to Protect, Detect, and React in Healthcare Cybersecurity

Creating comprehensive healthcare cybersecurity measures is essential for covered entities of all sizes. While technology continues to evolve, and facilities work to stay current, the online threats will also continue to evolve.

Organizations need to be prepared not only for insider threats and accidental breaches of information, but also for unauthorized access from malicious third parties. By using more connected devices, implementing BYOD strategies, and even connecting to HIEs, covered entities are also opening up the possibility for more exposure.

Healthcare cybersecurity measures must be current and well-rounded. Organizations need to not only detect potential threats, but also know how to protect against them, and how to react should an attack get through the system.

Protecting against potential attacks

One of the first key steps to strong healthcare cybersecurity measures is ensuring that your organization has the basic groundwork for protection in place. Tools such as firewalls, anti-virus software, and data encryption measures are all important areas to consider.

Reviewing the requirements for HIPAA technical safeguards is also a good place to start, as many of the common options for these safeguards can be key tools in protecting against possible threats.

For example, different types of authentication measures, such as multi-factor authentication can be beneficial. A password, PIN or passcode can help ensure that only authorized users gain access to sensitive information. Moreover, organizations can opt for login attempt limits, voice control features or even disabling speech recognition to improve authentication measures.

Data de-identification could also assist covered entities in keeping information secure. In this approach, certain identifiers are removed from PHI, such as patient names, telephone numbers, or email addresses.

As previously mentioned, data encryption is another tool that covered entities may want to consider. Encryption renders data unreadable by putting it into encoded text. Individuals will need the proper key or code in order to decrypt the information.

While not technically a requirement under HIPAA, data encryption is an "addressable" aspect. Essentially, HIPAA allows organizations to choose how and if they need to implement data encryption. However, with the increasing cybersecurity threats, data encryption is quickly becoming a more highly recommended tool for covered entities to adopt.

Detecting potential attacks

Being able to detect potential cybersecurity attacks is also crucial for healthcare organizations.

This can be done in several ways. First, employees should be fully trained on what to look for in terms of potential phishing or vishing attacks. Organizations can run a phishing scam exercise, to see if employees would fall for such an attack. From there, those individuals could be given extra assistance in knowing what to look for.

It is important that staff members are taught to look for simple things in an email, such as misspelled words, incorrect URLs or domain names, or even incorrect company logos. These could all be indications of a potential scam.

Employees also need to know who to contact should they detect something suspicious. Having a designated security team, or individual who is in charge of compliance and IT security can be beneficial.

Access control will also be critical for healthcare organizations in terms of detecting potential cyberattacks. Facilities should know who has accessed, or attempted to access, the network or areas where sensitive data may be stored.

This is another important aspect to HIPAA technical safeguards, and HHS requires organizations to "implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights."

Audit controls are another key tool for detection. This is when hardware, software, or other mechanisms that record and examine information system activity are utilized. However, the HIPAA Security rule does not specify the data that should be collected for audit controls or how often the information should be reviewed.

"A covered entity must consider its risk analysis and organizational factors, such as current technical infrastructure, hardware and software security capabilities, to determine reasonable and appropriate audit controls for information systems that contain or use ePHI," HHS explains.

Reacting to cyberattacks when they occur

The way that an organization reacts to a cyberattack is critical. If patient information has been compromised, for example, individuals have a right to be notified in a timely manner. Promptly notifying local and federal authorities is also important. No facility wants to delay the possibility of finding those who are responsible for a third-party attack.

According to the HIPAA Data Breach Notification Rule, covered entities and their business associates must notify necessary parties after unsecured PHI is compromised. This includes affected patients, the Department of Health and Human Services (HHS), and potentially the media.

For incidents that affect more than 500 individuals, notice must be given "without unreasonable delay" and in no case later than 60 days following the discovery of a breach. If less than 500 individuals are possibly affected, notice needs to be given in an annual report. Notices are also due to the Secretary "no later than 60 days after the end of the calendar year in which the breaches are discovered."

It is important to note though that regardless of a breach's size, individuals need to be notified without unreasonable delay or no later than 60 days following the breach discovery. Not only is this a federal requirement, but organizations will likely have a better chance at rebuilding their public reputation if they can show that a quick effort was made to tell individuals an incident took place.

Healthcare organizations cannot guarantee that a data breach or cyberattack will never take place. With the right tools and training though, facilities will have a better chance at protecting against possible attacks, detecting them, and if necessary, react to them.

Published by

About PC Connection, Inc.:

The PC Connection, Inc. family of companies has been trusted for more than 33 years to connect people with technology that enhances growth, elevates productivity, and empowers innovation. As a National Solutions Provider, our teams at PC Connection, GovConnection, and MoreDirect include experts who specialize in customized services and solutions for the healthcare market.

Learn more at: http://www.pcconnection.com/health