TechTarget SearchHealthIT

E-guide

PRO+ Content

Cybersecurity in Healthcare: 5 Best Practices

In this e-guide:

The increasing number of sophisticated attacks against health groups is putting CIOs and IT pros on high alert.

The ever-changing tactics used by attackers require everyone to adopt new and improved cybersecurity best practices, along with intelligent healthcare cybersecurity tech to keep patient data protected.

In this expert guide, discover:

- 5 best practices to help keep your environments safe from cyberattackers
- How health information management teams can help keep data secure
- A Q&A with security expert David Finn on how to build a successful cybersecurity program (even with a diminishing budget)

In this e-guide

5 healthcare cybersecurity best practices for care organizations

Reda Chouffani, Co-founder| Biz Technology Solutions

The increasing number of sophisticated attacks against health groups is putting CIOs and IT professionals on high alert. The ever-changing tactics used by attackers require everyone to adopt new and improved cybersecurity best practices, along with intelligent healthcare cybersecurity technology to keep patient data protected.

While end-user training and awareness are critical areas that continue to demand attention, there are several important steps that IT folks must address to ensure they're prepared to handle the changing threats lurking outside their environment. These healthcare cybersecurity best practices will help CIOs, CISOs and other security professionals to protect patient data and keep their environments safe from cyberattackers.

Get to know the network in depth. To implement the appropriate defenses and security protections, IT teams must ensure that they have an in-depth understanding of their network and attack surface. That'll expose the areas that attackers are likely to target and allow hospital IT to identify potential vulnerabilities. Hospitals have several devices and entry points in their systems that require cybersecurity best practices to protect a hospital environment. There are many tools, including Nmap, Netcat, Metasploit, Wireshark and NetworkMiner, that can create an inventory of hospital devices for the internet of things and mobile computing.

Adopt strong multifactor authentication. One of the more common healthcare cybersecurity practices is to require employees to use multifactor authentication (MFA) when connecting to hospital applications and systems. This practice ensures that leaked or stolen user credentials can't be used to gain access to internal systems without having access to additional details. MFA blocks many attacks resulting from stolen credentials by requiring users to present additional information to confirm their identity. MFA includes tokens, biometric methods and a code sent via text, email or voice.

Implement elevated privilege control. Security threats don't always come from the outside. In some documented security breaches, contractors or employees with elevated access have been the cause of leaked information. Administrators or contractors with elevated privileges present a logistical problem for hospitals since they often require more elevated forms of permission to do their work. As a result, a balanced approach that includes monitoring, temporary elevated access and audit trails ensures that adequate controls are in place for protection against these internal threats.

Adopt modern AI-based monitoring tools. Traditional security information and event management (SIEM) tools that simply monitor logs are no longer sufficient. The volume of information and the sophistication of today's attacks can easily go unnoticed by many of these traditional tools. Hospitals should adopt modern SIEM tools that use artificial intelligence and machine learning to analyze all the security events and traffic on a network and detect abnormal activities within the hospital environment.

Perform a thorough disaster recovery review. While hospitals continue to put safeguards in place to keep attackers at bay, it's critical that they be fully prepared if an attack requires restoring systems. CIOs acknowledge that their goal is to be attack-free, but there's still a chance that hospitals can fall victim to an attack despite their best security efforts. If that happens, their disaster recovery and business continuity plans are available and ready to be implemented.

CIOs and IT professionals in healthcare organizations recognize the importance of adapting their healthcare cybersecurity best practices in the face of constantly changing cyberthreats. Hospitals may not be fully prepared for the increasing volume of attacks, especially as attackers look to AI to increase their attack success rate. Fortunately, hospitals look to AI when it comes to fighting back -- and 2018 will certainly have its fair share of attacks.

↘ Next Article

In this e-guide

Health information management professionals aid cybersecurity

Tayla Holman, Site Editor

Hackers and cybercriminals continue to target the healthcare industry, leaving data at risk of exposure and being held for ransom. Cybersecurity remains a top priority for healthcare organizations, but figuring out how to manage and protect health information can be challenging.

Fortunately, health information management professionals are on the frontlines when it comes to protecting their organizations from attacks and securing patient data.

"Health information management professionals play a huge role in safekeeping PHI," said Shital Mars, CEO of Progressive Care, a health services company in North Miami Beach, Fla. "These individuals are tasked with knowing the vulnerabilities of their digital networks and assessing available solutions to secure their systems."

One of the main challenges organizations face is staying up to date with new cyberthreats and making sure that best practices for thwarting malicious intrusion and malware are followed, Mars said.

"For healthcare companies, the consequences of failing to protect systems are especially serious given the nature of the information and the regulations involved," Mars said.

One major consequence of failing to properly secure health systems and violating HIPAA is a hefty penalty. The Department of Health and Human Services recently upheld a finding from the Office for Civil Rights that required MD Anderson Cancer Center to pay $4.3 million in civil penalties for HIPAA violations.

By working together with the IT department, health information management professionals can help protect their organizations from attacks and secure patient data -- hereby avoiding those large fines -- said David Reitzel, principal and U.S. health IT leader at consulting firm Grant Thornton.

The IT department must make sure tools and software are properly configured to protect data and are scalable, Reitzel said. Then it falls on the health information management professionals to make sure that any hospital and patient data that is being shared is accurate.

"Both groups need to work collaboratively to ensure all the necessary policies, procedures and internal processes are reviewed and actively managed on a regular basis," Reitzel said.

Mars added that health information management professionals also need to be aware of new cyberthreats and should undergo regular training to stay in the know.

"Do continuing education on IT management throughout the course of the year to keep abreast of changing technologies and best practices," Mars said. "Read IT journals and news to make sure that all new threats are evaluated, the risks assessed, and solutions implemented."

Skills for health information management professionals

According to health IT consultant Reitzel, typical skills required in a digital health ecosystem include:

- data analytics and analysis capabilities;
- expertise in patient privacy and security rights; and
- understanding the scope of an organization's chief information security officer and chief information privacy officer.

"As health information technology continues to evolve, fluency in where patient data is shared outside of the organization, understanding of annual testing procedures, and the ability to manage and maintain databases and generate and analyze reports are critical," he said.

Health information management professionals also need to understand their organization's IT infrastructure so they know what systems need to be protected.

"It's important for anyone tasked with cybersecurity to understand the networks they work on and how those networks integrate, interface and communicate with both internal and external data sources like software providers, website hosts [and] email servers," Mars said. "By understanding the intricacies of your own network, you are best able to protect it."

Finally, Mars said, it is important to use best practices for keeping data secure, such as end-to-end encryption and multiple layers of password protection.

"Keep in mind there is no 'set it and forget it' when it comes to cybersecurity," Mars said. "As the healthcare industry adapts to better protect itself, [criminals] adapt as well, creating ever more sophisticated methods of obtaining data. So, for a health information management professional the job is never done."

➘ Next Article

Take commonsense approach to cybersecurity for healthcare plan

Dave Bernard, News Director | Business Applications & Architecture Media Group

In this Q&A, David Finn, executive vice president of strategic innovation at CynergisTek, a cybersecurity consulting firm, shares his views on how the dwindling number of insured is affecting cybersecurity efforts in healthcare and how a solution lies in a commonsense approach to cybersecurity for healthcare programs.

This interview has been edited lightly for length and clarity.

What do you see happening with insurance coverage and how does that affect cybersecurity for healthcare programs?

David Finn: [The number of] Americans without health insurance is up about 3.2 million people from 2017. That is concerning because it's the highest increase since 2008, which actually predated the implementation of Obamacare. Healthcare is about 18% of the economy, which is an unhealthy number for any single industry to consume that much of an economy.

Less insured lives mean less reimbursement for providers. At the end of the day there is no free healthcare. Someone is paying for it. Even if someone isn't covered, either on the marketplaces or they don't have their own insurance, those costs are going to be passed on or absorbed somehow, so the less money there is for patient care -- because the number of patients doesn't appear to be declining and the aging population is increasing -- there's going to be less money to do the other work of healthcare, the less important work, the back office work -- things like security and IT and interoperability, which would actually improve healthcare if we could spend the money on making the healthcare system more automated, more digitized and more efficient.

How can a successful cybersecurity for healthcare program be built, even with diminishing budgets?

Finn: This is one of the many things that has perplexed me for many years because it isn't rocket science. There is some technology needed, there are some skill sets needed. But one of the things I see is that a lot of organizations -- maybe they've just been through their risk assessments, or maybe they've had an event and they've decided they need to fix that particular issue around technology and the weaknesses they may have or the vulnerabilities they may have -- ... [decide] they have to fix everything all at once and that isn't how security gets built. You have to start with a vision of where you want to be. You have to decide what's important for your organization.

So you have to scale your security program and understand you're not going to fix everything all at one time. You have to prioritize those risks, determine what is most important to the organization, to the patient care, to the business of healthcare at that organization and then start building it.

I've seen organizations spend lots of money on bringing in tools to help them with security and then they realize they don't have the staff to maintain them or the people they've trained to do that have left the organization. You have to match your security program to your technology plan and strategy, and both of those have to be connected to the overall business strategy of the provider. And those are the disconnects I see most often: designing security to support IT and IT to support the business of healthcare.

What is the starting point for building a successful cybersecurity for healthcare program?

Finn: It's the one part of HIPAA that Congress and HHS got right, and that is starting with a risk assessment. But we tend to approach that as a technical security risk assessment, and that might have been fine when HIPAA was originally written because information technology wasn't as key to the business of healthcare. You could almost look at it as an IT and security issue. But today, the business runs on the EMR, it runs on your enterprise resource planning projects around inventory and payments and receivables. It runs on the clinical systems for placing orders and fulfilling those orders.

But we haven't made that adjustment in how we run the business. We don't think of that EMR as our core business operation, so in a lot hospitals, a lot of physicians practices, they still think of IT as something you do in addition to caring for patients. But these systems are now part of your operation.

So our risk assessment has to change from being, 'Oh, these ports are open and this system doesn't have the right password length,' to 'What happens when Epic shuts down? What happens when IT can't order X-rays because the [imaging] system is down?' So we have to shift that focus on risk assessment to not only security -- we still have to do that, we want everything to be secure -- but we have to consider it in terms of the impact to patient care, the quality of care and the clinical and business operations of the organization.

What is an example of a personnel-friendly approach to a cybersecurity for healthcare program?

Finn: Everyone has to have a designated security person. But the truth of the matter is you can have a chief information security officer, you can have a fully staffed information security department, you can have a wonderful governance structure -- but the technology risks come down to a personal level. People leave their machines logged on, people click on email that they shouldn't.

Every person in your organization, and not just employees but workforce members -- the volunteers, the visiting nurses, the doctors who come in -- everyone is part of your security team and has to be built into that, they have to be trained. I'll be the first to admit security training can be extremely dry and boring, so you have to engage everyone across the organization, and you have to do that in a way that is meaningful to them, that relates to them.

Everything you're doing in terms of security in your organization applies to them at home, it applies to the mobile devices they use. Sometimes they are using those mobile devices to interact with hospital resources and you don't control those end points as the security officer at the hospital. So it behooves all of us to make everyone more secure because everything is so interconnected. That's what I mean by personnel-friendly. And kind of building it in: You don't want to send people for three hours of security training on their first day. You're better off doing 15 minutes every month, and that can be web-based or an email or whatever, and it becomes top of mind so you have a personnel-friendly approach to it.

Where organizations use phishing exercises, we've seen security actually be enhanced. The hit rate for those phishing exercises dropped way down and very quickly. We've seen click-through rates of 60%, 70%, 80% drop very quickly down to 20% or less. And that's improved security without spending a lot of money or investing a lot of time.

And we could do that with other common attacks, making people aware of the issues, helping them understand it's not only the patient information they're protecting, but they're protecting their own information, they're protecting the hospital's information and they're making themselves more secure.

➘ Further Reading

In this e-guide

About SearchHealthIT

At SearchHealthIT, we provide free, unbiased news, analysis, and expert resources and for clinical and health IT professionals that manage healthcare operations for hospitals, medical centers, health systems, and other health organizations.

We know that patient care at your organization is your number one concern. That’s why we are dedicated to providing you with the tools, guides, strategies and techniques to improve efficiencies, cut costs, keep patient data safe, and meet regulatory requirements.

For further reading, visit us at http://SearchHealthIT.com/

Images; Fotalia