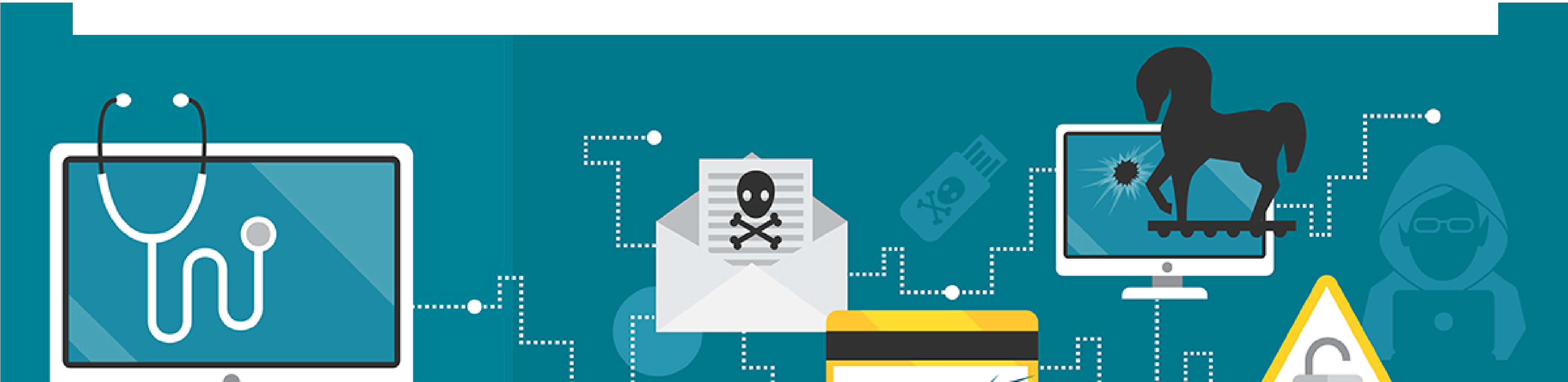
TechTarget | SearchHealthIT

E-guide

PRO+ Content

The Healthcare CIO's Guide to Cybersecurity



In this e-guide

Hospital cybersecurity isn't easy; CIO and CISO offer advice p.2

Learn how to detect cyberattacks and prevent them p.7

Cybersecurity of medical devices: The new threat landscape p.13

About SearchHealthIT p.17

In this e-guide:

In 2016, there were 284 reported healthcare breaches that each affected 500 or more individuals. The financial damage? Over $20 million in fines were assessed.

There's no magic bullet or single software that can fully secure your healthcare organization. But there are strategies that can help with cybersecurity.

In this e-guide, CIOs and CISOs from healthcare organizations across the U.S. share their tips. Learn from:

- Karl West, CISO at Intermountain Healthcare in Salt Lake City, Utah
- Hussein Syed, CISO at RWJBarnabas Health in West Orange, New Jersey
- Karen Clark, CIO at OrthoTennessee in Knoxville, Tennessee

In this e-guide

Hospital cybersecurity isn't easy; CIO and CISO offer advice p.2

Learn how to detect cyberattacks and prevent them p.7

Cybersecurity of medical devices: The new threat landscape p.13

About SearchHealthIT p.17

Hospital cybersecurity isn't easy; CIO and CISO offer advice

Kristen Lee, News writer

In 2016, cybersecurity attacks wreaked havoc in healthcare. Now that 2017 has rolled around, we can see the full impact these cyberattacks have had on healthcare and hospital cybersecurity.

According to a U.S. Department of Health and Human Services Office for Civil Rights breach report, in 2016 284 breaches were reported with 500 or more organizations and 15,106,367 individuals affected, and over $20 million in fines assessed.

And the picture only gets scarier with anyone having the ability to purchase ransomware online for $39, said Ladi Adefala, senior security strategist at Fortinet Inc., a cybersecurity software company based in Sunnyvale, Calif. He spoke during a session at the Healthcare Information and Management Systems Society (HIMSS) 2017 conference in Orlando, Fla. Adefala noted that also available is an option to purchase a "Russian Roulette" feature where files are deleted every six hours until the victim pays the ransom.

And you never know where cyberattacks might come from. An audience member shared that malware was introduced into his healthcare organization's environment via an e-cigarette.

In this e-guide

Hospital cybersecurity isn't easy; CIO and CISO offer advice p.2

Learn how to detect cyberattacks and prevent them p.7

Cybersecurity of medical devices: The new threat landscape p.13

About SearchHealthIT p.17

Suffice it to say, multiple health IT experts, including CIOs and CISOs, said at HIMSS 2017 that hospital cybersecurity is at the top of their list.

Network segmentation for hospital cybersecurity

Hussein Syed, CISO at RWJBarnabas Health located in West Orange, N.J., suggested that healthcare organizations look into network segmentation, a long-time security strategy that essentially separates networks based on who or what they serve, something Hussein has implemented at RWJBarnabas.

"We have urgent care, we have physicians' offices, we have specialty hospitals and we have outpatient clinical ... and they're all connected together to a central EHR," he said. "All those points of entry can lead to ransomware, malicious malware ... into that environment."

Syed said now that new technologies are being introduced into healthcare organizations that allow for remote access, and for providing care outside the hospital and in the patient's home -- such as telemedicine -- the area of risk has widened.

"Now we have physicians, caregivers, remote workers, you name it, all over the country reporting in or accessing the four walls and doing the work and really trying to do what they need to do and now bring in extra threats," Syed said.

In this e-guide

- Hospital cybersecurity isn't easy; CIO and CISO offer advice p.2
- Learn how to detect cyberattacks and prevent them p.7
- Cybersecurity of medical devices: The new threat landscape p.13
- About SearchHealthIT p.17

Syed suggested that healthcare organizations segment their network into smaller networks dedicated to one function. For example, creating a business network and a clinical network and a network for medical devices and the EHR.

"This way if one environment is compromised at least you can contain that infection, that threat, into that little environment," Syed said, adding that these various network environments can be assigned a risk rate based on which environments are at a higher risk and which are at a lower risk.

Syed suggested that when healthcare organizations decide to embark on a network segmentation project that they adopt a framework, perform focused risk assessments, develop a strategic plan of three years or more, and focus on incident response.

Since segmenting their network, Syed said RWJBarnabas has experienced several benefits:

- Seventy percent increased patient and physician satisfaction due to improved public internet access;
- Forty percent true security events compared to 67% false positives;
- Thirty percent increased visibility into advanced persistent threat activity; and
- Seventy-five percent financial savings by avoiding architectural footprint in the virtual environment.

In this e-guide

Hospital cybersecurity isn't easy; CIO and CISO offer advice p.2

Learn how to detect cyberattacks and prevent them p.7

Cybersecurity of medical devices: The new threat landscape p.13

About SearchHealthIT p.17

Prep for when a user clicks on a malicious link

Karen Clark, CIO at OrthoTennessee in Knoxville, Tenn., said simply training end users about what not to click on is not enough for a hospital cybersecurity strategy.

"We could train every one of our 700 users perfectly, and 699 of them get it and one person was sick that day or just didn't pay attention and that one person clicks on a piece of ransomware," Clark said.

Clark advised that healthcare organizations identify what systems would be highly affected should they be hit by ransomware and focus their resources there.

Since it's highly likely a user is going to click on a malicious link or open a malicious email, and the results could end up with a healthcare organization's entire database being encrypted, Clark said, "that's where I'm going to put resources."

Clark gave an example of what protections she would put in place in this scenario.

"I'm going to put protections in place at the perimeter to control and prevent certain types of inbound and outbound traffic and I'm going to be sure that, for example, I do hourly backups of my major database with log shipping to a separate encrypted device that's not ... a network share," she said. "So that if a user clicks on a file, it can only affect their computer. But if it escapes that

In this e-guide

Hospital cybersecurity isn’t easy; CIO and CISO offer advice p.2

Learn how to detect cyberattacks and prevent them p.7

Cybersecurity of medical devices: The new threat landscape p.13

About SearchHealthIT p.17

defense and encrypts my main database, then I just go to my backup from an hour ago."

Have an independent security risk assessment

Clark recommended that healthcare organizations not use security vendors to conduct risk assessments. Instead, find a trustworthy third party, she said.

"One of the things we did at OrthoTennessee is partnered with our local FBI field office because the FBI has great resources for cybercrime," Clark said.

Clark and her colleagues met with their local FBI office and told them about their cybersecurity efforts, asked them for feedback, and asked them what cybersecurity activity the FBI is seeing in the healthcare space.

"They don't have a vested interest in what you buy but they're really good at what they do," Clark said.

↘ Next article

In this e-guide

Hospital cybersecurity isn't easy; CIO and CISO offer advice p.2

Learn how to detect cyberattacks and prevent them p.7

Cybersecurity of medical devices: The new threat landscape p.13

About SearchHealthIT p.17

Learn how to detect cyberattacks and prevent them

Kristen Lee, News writer

With ransomware attacks increasing 300% in little more than a year -- from 1,000 daily attacks in 2015 to 4,000 in early 2016, according to a U.S. government interagency report -- it's no wonder cybersecurity is top-of-mind for many health IT professionals.

While it's important to train and educate healthcare employees on best practices to keep the organization secure, "we're not going to solve this issue just by educating our workforce," said Mac McMillan, co-founder and CEO of CynergisTek Inc., a healthcare IT consulting firm in Austin, Texas. The right technologies to prevent, detect, resist and recover from an attack are essential to maintaining security and keeping a healthcare organization up and running.

Technology to prevent cyberattacks

Using effective technologies to *detect* cyberattacks is important, but security professionals say healthcare organizations need to use technologies designed to *prevent* attacks as well. Many good technology options are available to do just that.

In this e-guide

Hospital cybersecurity isn't easy; CIO and CISO offer advice p.2

Learn how to detect cyberattacks and prevent them p.7

Cybersecurity of medical devices: The new threat landscape p.13

About SearchHealthIT p.17

Multifactor authentication. McMillan advised that healthcare organizations use at least two-factor authentication. In addition to having a username and password, employees should have another layer of credentials, such as a security question, electronic token or biometric authentication like a thumbprint. Doing so creates barriers for anyone seeking unauthorized access to an account.

"That just makes it that much harder because you might have my phone; you may even guess my password," said McMillan, who spoke at the annual American Health Information Management Association conference in Baltimore last October. "But you're not going to have my [thumbprint], and you're not going to have my token."

David Reis, senior vice president and CIO at Lahey Health in Burlington, Mass., agreed, adding that more hospitals need to follow this approach. Although encryption has become standard in healthcare, multifactor authentication has not. Such authentication for remote access is particularly important, he said.

Healthcare organizations that allow remote access to systems should insist on a username and password for each user as well as a PIN that changes every 30 to 60 seconds, Reis said. This step would apply to remote users of email, ERP systems, patient portals or clinical applications such as electronic health records.

"This type of security technology would have largely prevented the email breaches that we've been seeing in the media where someone gets successfully phished, giving up their user credentials, and then the bad actor

In this e-guide

Hospital cybersecurity isn't easy; CIO and CISO offer advice p.2

Learn how to detect cyberattacks and prevent them p.7

Cybersecurity of medical devices: The new threat landscape p.13

About SearchHealthIT p.17

logs in and accesses emails with patient information," Reis explained. "This scenario is exactly the kind of thing that multifactor authentication prevents from happening in almost every case."

Behavioral analytics. Using data to measure employee behavior can also help tighten security. If healthcare employees -- doctors, nurses or residents -- have access to a system, McMillan said, they usually can view information about all the patients in that portion of the healthcare organization's system.

However, some technologies can monitor how employees use those systems and track what information they access. For example, if a doctor in the emergency department looks up a patient's information in the oncology ward, that action would trigger an alert to the IT department because the doctor may be accessing information he doesn't necessarily need, McMillan said.

"We need to start normalizing behavior across platforms and across positons so that we understand what is normal for [a clinician] to look at in a given day," McMillan said. "And if he's looking at [50%] or 100% more information than is normal for him to look at, that should set off a flag, too, even if he's still within his lane. We need those behavioral analytics."

Honeypot. McMillan said another option to prevent attacks is to install a honeypot, which essentially creates a fake server that will lure attackers "and cause them to waste time playing around out there as opposed to actually hacking your network." Healthcare organizations should set up their honeypot so that they can track and block the IP address of the attackers.

In this e-guide

- Hospital cybersecurity isn't easy; CIO and CISO offer advice p.2
- Learn how to detect cyberattacks and prevent them p.7
- Cybersecurity of medical devices: The new threat landscape p.13
- About SearchHealthIT p.17

How to detect cyberattacks with technology

An effective way to detect -- and protect against -- ransomware or cyberattacks is to have next-generation firewalls and security email gateways work together, Reis said. "What that interoperability between firewalls and security email gateway devices would do is identify that something was running in the environment that looked suspicious and then inspect email attachments for known patterns, ... not in an antivirus way, [but] in a crowd-sourced way," he explained. Like the internet of things, security tools would be aware of what other security devices are discovering, he noted, adding that "this is similar to intrusion detection and prevention solutions but with a different focus."

Technology to respond to a cyberattack

When it comes to meeting an attack head on, some hospitals succeed with advanced persistence threat (APT) technologies, said Mark Dill, a partner and principal consultant at tw-Security, a healthcare security firm based in Strongsville, Ohio. According to Dill, APT looks for early infections in the network that ultimately become ransomware problems.

In this e-guide

Hospital cybersecurity isn't easy; CIO and CISO offer advice p.2

Learn how to detect cyberattacks and prevent them p.7

Cybersecurity of medical devices: The new threat landscape p.13

About SearchHealthIT p.17

He advised that healthcare organizations put APT technologies in block mode, which halts the communication between the malware and the organization's command control server. This defense is important because communication is sometimes necessary for the malware to get the encryption key to actually encrypt the data. But with block mode, Dill said, the technology can prevent the encryption key from ever getting into the organization. "It gives IT and antivirus software a chance to catch up and figure these things out," he explained.

Hospitals, grab your bitcoin wallet

Should a healthcare organization experience a cyberattack or ransomware attack, having a bitcoin wallet makes the recovery process much quicker if the organization has no choice but to pay the ransom, said Mark Dill, partner and principal consultant at tw-Security, a healthcare security firm based in Strongsville, Ohio.

A slew of healthcare organizations suffered through ransomware attacks in the past few years and were forced to pay, including New Jersey Spine Center in Chatham, N.J.; Marin Healthcare District in Greenbrae, Calif.; Kansas Heart Hospital in Wichita, Kan.; and Hollywood Presbyterian Medical Center in Los Angeles.

Without a bitcoin wallet, which is basically a bank account that holds a person's or organization's bitcoin currency, it could take up to a week for the traditional money to transfer, Dill said. Such a delay prolongs the return of the healthcare organization's data and, in some cases, could cripple hospital

In this e-guide

Hospital cybersecurity isn't easy; CIO and CISO offer advice p.2

Learn how to detect cyberattacks and prevent them p.7

Cybersecurity of medical devices: The new threat landscape p.13

About SearchHealthIT p.17

operations. With a bitcoin wallet, the transfer of the ransom currency is much faster.

Recovering from an attack

Despite knowing how to detect threats and using technologies to prevent ransomware and cyberattacks, healthcare organizations should also have a recovery plan. One method is to back up data frequently so a hospital can restore that data and keep functioning after an attack. But Dill also pointed to the data center as a way to recover.

First, he advised that healthcare organizations invest in tiered storage, in which the most frequently accessed data is stored on higher-performing storage devices and rarely accessed data is put on low-performance, cheaper storage. Tier-two storage, in particular, is important because "a tier two starts to have some redundancy [of data] and some of the controls," Dill said. If a healthcare organization is hit by a ransomware attack, those features would make it possible to recover some of the data held hostage.

He also recommended that hospitals set up their data centers so they're redundant. That means if one data center experiences a disaster -- be it a ransomware attack or hurricane -- the healthcare facility would have all that data stored in another data center. In that way, Dill explained, healthcare organizations could do what he called a "data center flip-flop," adding "where my system is so good that I can run for a month in a data center 15 miles away and then one night fail it over to the other data center."

In this e-guide

- Hospital cybersecurity isn't easy; CIO and CISO offer advice p.2
- Learn how to detect cyberattacks and prevent them p.7
- Cybersecurity of medical devices: The new threat landscape p.13
- About SearchHealthIT p.17

Cybersecurity of medical devices: The new threat landscape

Kristen Lee, News writer

Karl West believes "medical devices are the new threat landscape."

The CISO at Intermountain Healthcare in Salt Lake City, Utah, explained that the influx of medical devices into health organizations, often without the knowledge of IT, may be adding to existing security problems. Experts agree that precautions concerning the cybersecurity of medical devices need to be taken on the part of the provider and the medical device manufacturer.

West explained that compared to the number of more traditional vulnerabilities within a healthcare organization -- such as endpoints like computers vetted by IT -- there are seven or eight times more medical devices which usually do not pass through the IT department first.

"What most healthcare [organizations] are doing right now is trying to wrap their arms around this new risk," West said. "It's significant."

Experts said while one concern is that these devices usually don't enter an organization's environment through the IT department -- West explained they usually come in directly through specific departments such as ophthalmology or anesthesiology -- another concern is that the U.S. Food and Drug Administration's (FDA) guidance when it comes to medical device security is lacking.

In this e-guide

- Hospital cybersecurity isn't easy; CIO and CISO offer advice p.2
- Learn how to detect cyberattacks and prevent them p.7
- Cybersecurity of medical devices: The new threat landscape p.13
- About SearchHealthIT p.17

The FDA's medical device guidance and post-guidance

West and Mike Nelson, vice president of Healthcare Solutions at DigiCert, a security certification company located in Lehi, Utah, explained the FDA's medical device guidance used to focus mainly on patient safety and, while patient safety is important, at the moment many in health IT are more concerned about securing healthcare organizations and protecting them from data breaches.

"We're concerned about vulnerability, task management, the ability to keep these devices current, to scan them for virus[es] and malware," West explained.

But because the FDA's guidance is used to focus on patient safety and not on critical security protocols that medical device manufacturers should be taking, both West and Nelson explained, the manufacturers had no motivation to implement security features such as updates or patching.

However, the FDA recently released its Postmarket Management of Cybersecurity of Medical Devices guidance which the experts believe will help push manufacturers to better update and patch their devices.

"I think manufacturers have used the FDA potentially imposing additional regulatory burdens as a reason for not updating and doing patch management with their existing devices," Nelson said. "But the FDA has now cleared this impediment."

In this e-guide

Hospital cybersecurity isn't easy; CIO and CISO offer advice p.2

Learn how to detect cyberattacks and prevent them p.7

Cybersecurity of medical devices: The new threat landscape p.13

About SearchHealthIT p.17

In other words, the postmarket guidance clarifies the FDA requirements for manufacturers therefore there is no reason for manufacturers to not update devices and outfit them with the correct security protocols.

However, West doesn't think the postmarket guidance is enough and that it still focuses too much on patient safety and not enough on what many in healthcare are worried about which are data breaches and data loss.

West said the guidance needs to not only address that these devices sitting in a hospital's environment are a potential threat to patient safety but also to the patient's data and protected health information. "That wasn't addressed or even discussed with respect to access to patients' data," West said.

Precautions providers can take

While it may seem that the security of medical devices is out of the provider's hands -- since it's up to the manufacturer to put the correct security protocols in place on the device itself -- West said providers can take steps to better ensure the cybersecurity of medical devices.

The first step is for providers to take inventory of all the medical devices that exist in their environment. West said it can take some time to find all the devices that may have crept into a healthcare organization from so many different places.

Once a healthcare organization has -- hopefully -- found every medical device in its organization, then it can assess the risk of each device.

In this e-guide

Hospital cybersecurity isn't easy; CIO and CISO offer advice p.2

Learn how to detect cyberattacks and prevent them p.7

Cybersecurity of medical devices: The new threat landscape p.13

About SearchHealthIT p.17

"Which means you've got to classify the data that's on those devices," West said. "What kind of data is being stored? Is it persistent? Is it static? Is it dynamic? What is the category of risk that we assign to the device based on the understanding of data and location and then motion of data?"

Once the assessment of risk for each device has been made West said the next step is to identify what security controls exist, if any.

"In fact, many of the devices that are in the hospitals came out before the guidance that we've referenced," he said. "So there may or may not be any controls. And by controls what I'm talking about is the ability to put a password on, ability to put encryption on the device, [and] ability to update and manage the vulnerabilities."

Next article

In this e-guide

Hospital cybersecurity isn't easy; CIO and CISO offer advice p.2

Learn how to detect cyberattacks and prevent them p.7

Cybersecurity of medical devices: The new threat landscape p.13

About SearchHealthIT p.17

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