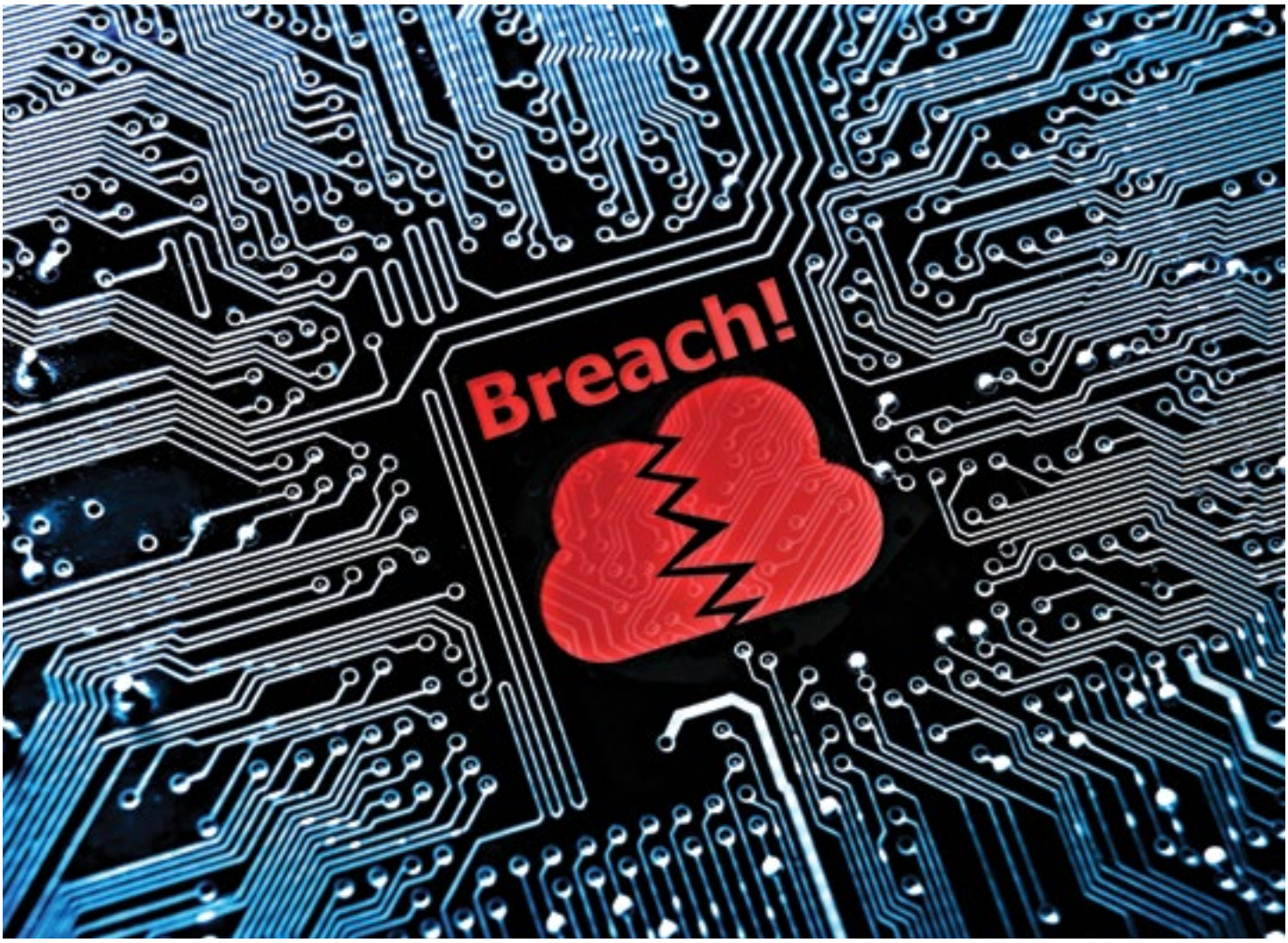

NOT IF BUT WHEN:

PREVENTING THE NEXT GENERATION OF SECURITY ATTACKS IN HEALTHCARE

HEALTHCARE INFORMATICS
CUSTOM MEDIA

RESEARCH SUPPORTED BY:

PC Connection
MoreDirect
A PC CONNECTION COMPANY

Contributing Executives

Phil Curran
Chief Information Security Officer and Chief Privacy Officer
Cooper University Healthcare

Phil Curran has more than 20 years of experience in information security and privacy in the military, government and private sectors. As the Chief Information Assurance and Privacy Officer at Cooper University Health Care in Camden NJ, he is responsible for managing governance and regulatory compliance, risk assessment and management, threat intelligence and vulnerability assessment, privacy and security investigations, business continuity, and awareness & training.

Ron Mehring, MBA, CISSP
Vice President of Technology and Security
Texas Health Resources

Ron Mehring serves as the vice president of Technology & Security for Texas Health Resources, one of the largest faith-based, nonprofit health care delivery systems in the United States. The system's primary service area includes 16 counties in north-central Texas, home to more than 6.2 million people.

At Texas health Resources, Ron leads Technology Operations, IT Risk Management & Assurance, IT BC DR program and Technology & Security Performance and Standards teams.

Ron began his career in technology for the United States Marine Corps. After 21 years of military service, Ron retired from the Marine Corps and joined the Department of Veteran Affairs where he led Compliance Assessment teams within the newly formed Oversight & Compliance group. He also served as the Department of Veterans Affairs' Deputy Director for Network & Security Operations.

Ron holds a Master of Business Administration in Risk Management from NYIT and is a Certified Information Systems Security Professional (CISSP).

Martin Littmann
Chief Technology Officer and Chief Information Security Officer
Kelsey-Seybold Clinic

As Chief Technology Officer and Chief Information Security Officer at Kelsey-Seybold Clinic, Martin Littmann has led the expansion of the depth, breadth, and scope of the IT organization there. He has spear-headed efforts to improve quality and efficiency across the data center, network, and information security domains to implement, expand, and sustain clinical and administrative objectives in EMR (Epic), ERP (Lawson), PACS (Brit), and administrative (Lawson, Kronos) application areas.

Littmann has proven to be a demonstrated hands-on expert in developing and cultivating organizations, educating and engaging executive leadership, and building strategic customer and vendor relationships critical to the organization's success.

Stephen Nardone
Practice Director of Security and Mobility
PC Connection, Inc.

Stephen Nardone is an industry-leading security expert with more than 35 years of experience in security program development and management, risk governance and oversight, architecture, service development and delivery, and security vulnerability management, assessment and testing. As Practice Director of Security and Mobility, Nardone leads the Company's efforts to develop solutions and services that help customers reduce exposure to security threats. Prior to joining PC Connection, Inc., Nardone worked at the National Security Agency (NSA) for 15 years, where he ran NSA's Commercial Trusted Product Evaluation Program. Nardone also served as CSO/CTO of the Commonwealth of Massachusetts, and held various leadership positions in the private sector on both the Professional Services and Operational Security side. He is a member of the International Information Systems Security Certification Consortium (ISC)2, Information Systems Security Association (ISSA), Institute for Electrical and Electronics Engineers (IEEE), and InfraGard. Nardone holds a BSEE in Electrical Engineering from University of Lowell.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The costs of healthcare data breaches are staggering.

Over the past few years, healthcare organizations such as New York-Presbyterian Hospital and Columbia University,[i] Cignet Health,[ii] and Blue Cross Blue Shield of Tennessee[iii] have paid millions of dollars in data breach settlements. But the costs go far beyond those fines. Blue Cross Blue Shield Tennessee estimates it paid out over $17 million in "investigation, notification, and protection efforts" after its breach caused by the theft of unencrypted hard drives.[iv] And that amount is before the organization can consider the long-term impact, and associated costs, of lost trust and confidence by the larger patient community.

Blue Cross Blue Shield Tennessee estimates it paid out over $17 million in "investigation, notification, and protection efforts" after its breach caused by the theft of unencrypted hard drives.[iv]

Cybersecurity is more than just a buzzword. It is a key competence that needs to exist beyond the cubical walls of a hospital's IT department with strategies and policies in place that extend across the entire enterprise. But with new and more sophisticated attacks on the horizon, it can be difficult for healthcare organizations to understand how to best protect their patients—and their business.

The purpose of this research report is to better understand how healthcare organizations can better prepare for the next generation of cyber security attacks. This report will discuss the current security threat landscape, including spear phishing attacks and ransomware, and how cybersecurity experts see those threats evolving over the next few years. It will outline the healthcare-specific challenges involved in putting in place a sustainable cybersecurity plan. It will consider why it is so important for healthcare organizations to be open and transparent about cybersecurity strategies across the enterprise. And, finally, it will highlight the workflows and processes required to help healthcare organizations of any size take better control of security endeavors and defend the enterprise against increasingly sophisticated attacks, helping your organization to protect critical protected health information (PHI), reduce the risk of extravagant fines, and increase patient trust.

INTRODUCTION

$1.2 million. $1.7 million. $3 million. $4.8 million.

The numbers are staggering. So much so that you might think these figures might represent some additional budgetary allotments for new and innovative information technology (IT) projects. But they are not. They are the dollar amounts of data breach fines and settlements that various healthcare organizations have paid out over the past few years for violating the Health Insurance Portability and Accountability Act (HIPAA). They represent the price of a deactivated network server that made patient data accessible online. The cost of stolen portable storage devices or unencrypted laptops. The bill for returning a photocopy machine without first wiping the hard drive clean of patient data.[v] The price of not safeguarding protected health information (PHI) at all costs.

But the costs don't stop at fines and settlements. A Ponemon research report stated that the additional expenses related to a data breach are also substantial. Given the expenses related to incident handling, organizations can expect to pay approximately $233 per compromised record—and that's without considering the expenses involved with recovery actions such as data recovery and legal fees.[vi] Blue Cross Blue Shield of Tennessee estimates it paid out in excess of $17 million in related expenses after its well-publicized theft of unencrypted hard drives filled with PHI.[vii]

"It's easy to find a financial motivator here and help educate others so they see that information security activities are a form of insurance that we need to be keeping."
– Martin Littmann

Martin Littmann, Chief Technology Officer and Chief Information Security Officer for Kelsey-Seybold Clinic, says he uses the news stories about these breaches and associated costs to help educate clinicians and other key stakeholders about the importance of cybersecurity.

"I regularly send around news stories of other people that have had fines levied against them," he says. "Seeing the outcomes from various investigations that result in these kinds of fines for breaches whether due to poor behavior, poor practices, or poor policies helps them see the value. It's easy to find a financial motivator here and help educate others so they see that information security activities are a form of insurance that we need to be keeping."

Stephen Nardone, Director of Security and Mobility Professional Solutions and Services Practice at PC Connection, Inc., agrees that such public fines and settlements are providing an important service as a warning to healthcare entities of what can happen when breaches occur.

"A lot of the healthcare organizations we talk to seem to be a little bit behind the power curve from where they need to be when it comes to having a good set of security controls and procedures to help protect their electronic protected health information (ePHI)," he says. "We're seeing interest grow because of these kinds of fines but also because the number of attacks, the types of ransomware we've been seeing over of the past six to eight months, are increasing, too."

Cybersecurity experts across the industry agree. When it comes to cybersecurity threats, it's not a matter of if, but when. Hospitals and other healthcare organizations should expect to be attacked.

"The number one thing you need to realize is that, no matter what you do, you're going to get broken into eventually. If someone really wants to break in, they are going to find a way in," says Ron Mehring, Vice President of Technology and Security at Texas Health Resources.

"The number one thing you need to realize is that, no matter what you do, you're going to get broken into eventually. If someone really wants to break in, they are going to find a way in," – *Ron Mehring*

Yet despite this reality, according to several surveys, healthcare organizations are not investing enough in their cybersecurity programs.[viii] To survive those cyber-attacks, and offer patients the highest quality care and privacy, Mehring argues, this needs to change. Healthcare organizations need to prioritize information security investments in order to create and maintain a transparent, effective security plan to appropriately respond to such break-ins so that patient data—and subsequent patient care—are not at risk.

THE THREAT LANDSCAPE —NOW AND IN THE FUTURE

Today, most hospital information security officers are concerned about the prevalence of ransomware attacks, a form of malware that locks down an organization's network and prevents the access of data until a ransom, usually demanded in Bitcoin, is paid. A recent quick-hit survey conducted by the Healthcare Information and Management Systems Society (HIMSS) found that 75% of respondents had been hit with some form of ransomware attack in the past year.[ix] And a Wired magazine article published in March of 2016 suggested that hospitals are a preferred target for such cybersecurity extortion because they rely on patient information to provide the best quality care.[x] Indeed, any ransom demanded would almost certainly cost less than a rash of patient injuries and deaths—and the resulting malpractice lawsuits.

"The threat is there. But it's not just ransomware," says Nardone. "It's estimated that the value of a healthcare record is 10 times the value of a credit card in the open market. And that's why individuals are specifically targeting hospitals in general looking for ways to breach the system. That patient data has a lot of value, whether they are trying to access it or hold it hostage."

A recent quick-hit survey conducted by the Healthcare Information and Management Systems Society (HIMSS) found that 75% of respondents had been hit with some form of ransomware attack in the past year.[x] – *HIMSS*

He says that healthcare organizations are now also having to deal with polymorphic malware, a piece of code with intelligence to change and morph within the system to avoid detection, as well as with maintaining the physical security of computers, laptops, thumb drives, and other mobile devices. He also says that hospitals need to consider how they will manage the security of medical devices—physical devices such as pacemakers that may be sending data to and receiving data from the electronic health record (EHR) system.

"There's a lot that's out there," he says. "And the best process to follow is to be prepared for any sort of attack—and really just expect that it is going to happen. Build your process and your program around the fact that an attack will happen."

Ron Mehring, Vice President of Technology and Security at Texas Health Resources, says that even traditional "spear phishing" or "phishing" attacks, where a seemingly legitimate email attempts to convince an employee to click a malicious link in order to gain access to the network, can have severe consequences. He says what some call "old" attacks are evolving—and an organization's response plan needs to be just as agile to deal with such threats.

"People call things the 'next generation' attack but they all seem to be rebranding of old attacks. The way attacks are performed, I think, won't change dramatically over the years," he says. "Attackers will find different ways to exploit and access the infrastructure and you need to be able to react to that. And as the controls are getting better, our adversaries are having to get better at what they do. So we have to get better, too."

OUTLINING THE LATEST THREATS

RANSOMWARE

Modality: An attacker gains access to a network via phishing or a physical entry point (USB stick), installing a virus that encrypts files that can only be unlocked via a specific passcode or key. The attacker establishes contact and demands a ransom payment, typically in Bitcoin.

Prevention Methods: Identify and define value of critical data and where it is housed within the network, understand protection protocols and access governance of this data, understand firewalling and encryption practices for high-value data, add a DMARC or filter for email systems, run continuous mock scenarios against clinicians and administrative staff illustrating a potential attack, create "live" scenarios for IT teams specifically to isolate and eliminate ransomware threats.[xi] **More specific steps:** avoid mapping drives and hide network shares, delegate record write access only when needed, explore and research CryptoLocker Software Restriction Policies, always have working and reliable data backups, be aggressive in blocking file extensions via email, use application whitelisting to prevent unapproved programs from running[xii].

Meet the Ransomware Family (The Well-Known Variations of Ransomware):
CryptoLocker, Locky, TeslaCrypt, CryptoWall, Samas

SPEAR PHISHING

Modality: An attacker crafts and sends an email to a carefully selected target group that prompts the user to download a malicious attachment or share sensitive data. Emails are typically personalized to mimic that of an email the target would typically receive, which includes official email signatures, logos, or similar email address domains. Content of the email can also be driven by social engineering and data mining of online profiles (Facebook, LinkedIn, etc.). Credentials are then used to access sensitive data, create additional backdoors for access to the network, steal valuable records, and erase activity log records.

Recently Impacted Organizations:
Main Line Health[xiii], CareFirst[xiv]

Prevention Methods: Advanced end user education focusing specifically on limiting a target's potential online exposure through social media or websites, advanced password requirements for network users, dual-factor and strong authentication for access to critical systems, closely managing patches and updates to security software, create internal mock phishing attacks to continuously test network penetration and employee training.

WHALING OR CEO FRAUD

Modality: An attacker sends an email request from a C-Suite executive, director, or management team member either through a compromised email address or through a false email address requesting immediate money transfers to an external account.

Prevention Methods: Continuous C-Suite penetration testing and monitoring, initiate test phishing campaigns targeting C-Suite executive team members, application of advanced email phishing filters, crafting verification processes upon receiving financial requests (phone verification, etc.), arrange educational meetings and programming targeted for C-Suite executives and their administrators.

OUTLINING THE LATEST THREATS Continued

DOMAIN SPOOFING

Modality: An attacker uses a phishing email to redirect a user to a falsified domain website, which mirrors or mimics similar functionality to that of an internal company website. Often the initial phishing email will appear as an official system generated email directing the user to a portal for entry of credentials or sensitive information.

Prevention Methods: Configure mail gateways or firewalls to use LDAP lookup to confirm the existence of email recipients, configure mail server to block email from open relay blacklists or DNS blacklists, leverage authenticated mail relays[xv], format systems to authenticate domain names, launch education initiatives among employees about falsified domains, continue penetration tests with falsified domain website scenarios among staff and C-Suite team.

POLYMORPHIC MALWARE

Modality: An attacker gains access to a network via phishing or on-site access and installs a malware program (Trojan, worm, virus, etc.). This virus then is able to evade security countermeasures and firewalls by continuously rewriting and manipulating files to change and hide its appearance within a system. Oftentimes adapted from threats originally attacking the banking industry.

Prevention methods: Threat scenario testing with IT team members, develop an isolation plan for infected machines from the network, develop and install advanced security threat detection software combined with robust server level monitoring, advanced training for employees in both on-site security and email security to limit risk, invest in and hire IT staff members that specialize in targeting, detecting, and eliminating advanced security threats.

UNDER THE MICROSCOPE:

THE ANATOMY OF A NEXT-GENERATION THREAT ON THE HORIZON SHIFU TROJAN –

Currently a high-powered threat used to attack the banking industry, Shifu is a next-generation malware developed using components of the Shiz, Gozi, Zeus and other well known viruses. Upon infection this Trojan variation wipes local system restore points, is an XML format which limits its exposure to security systems and protocols, disables security tools and sandboxes, steals authentication tokens and can forge user certificate keys. Shifu is also one of the first malwares seen with active security measures built in to prevent other malware from entering the system, to allow continuous control of its environment. A basic Shifu Trojan can become a very dangerous potential risk for healthcare providers, and includes the following stock features:

- Anti-research capabilities
- Browser hooking and web inject parsing
- Certificate grabbing
- Screenshot grabbing
- Remote access tools (RAT)
- And more…[xvi]

THE CHALLENGES OF CYBERSECURITY IN THE HEALTHCARE SPACE

Curran says the unique aspect of healthcare cybersecurity is the focus on the patient. "We need to be aware of any security issue that may affect the patient or have a negative impact on patient care," he says. "The data in an EHR is critical. If you can't access it, or the data is wrong, you could potentially kill a patient. So our security always has to center around the patient."

And, certainly, the street value of a complete healthcare record makes hospitals a unique target for cyberattack as well. But are hospitals ready? In 2014, Reuters reported that the FBI had sent a special memo to healthcare providers warning them that their cybersecurity protocols lagged behind those found in other industries, making them more vulnerable and more likely to be targeted by cyberattacks.[xvii] Mehring says he doesn't think all healthcare organizations are lagging behind—but he does say that healthcare faces some challenges that make it more difficult to put strong security strategies in place.

"As the Internet of Things (IoT) gets bigger, we're going to have medical devices that are going to be part of the medical record. Maybe not too far in the future, we'll have implantable devices that automatically monitor your heart rate and add that data to your electronic health record. We need to start thinking now about how we can protect those medical devices." – *Phil Curran*

"It's a complex world. Whether you're on the payer, provider, or medical device side. You have a lot of complex architectures and complex systems," he says. "You have old systems that have been around for many years that we've carried forward because they work well and they are tightly integrated with clinical workflows. So you have those old systems interacting with new systems as we bring in new capabilities. That interaction of old and new—we carry a lot of agents in one collective network. It can get really complicated."

Phil Curran says that some of those newer agents that require careful security monitoring are mobile and medical devices. "As the Internet of Things (IoT) gets bigger, we're going to have medical devices that are going to be part of the medical record. Maybe not too far in the future, we'll have implantable devices that automatically monitor your heart rate and add that data to your electronic health record," he says. "We need

to start thinking now about how we can protect those medical devices. You need to mitigate the risks as much as possible."

Mehring says that means there are a lot of things for a healthcare organization to keep track of—and the list will just keep getting longer.

"You have so many different things piling into the architecture. The complexity just keeps building," says Mehring. "And all these different surface areas create opportunities for malicious actors. It's hard to address them all at the level of robustness necessary to keep every bad person out."

Education and People Management

And there is one particular surface area that requires extremely careful management when it comes to cybersecurity: a healthcare organization's own employees. In 2012, a Trend Micro report suggested that 91% of all cyberattacks across industry verticals start with a simple phishing email.[xviii] And the 2016 Verizon Data Breach Investigations Report found that, on average, 11% of end users click on included attachments in phishing messages.[xix] While these reports focused on all industry verticals, Littmann says it's important to understand healthcare is not immune to such risks.

"The first time I sent a phishing email campaign out in my organization, to test our risk, the results shocked both me and our executive team in terms of the gap in our security awareness and education. It became an area of emphasis for us." – *Martin Littmann*

"You need to understand where your highest security risks are. And you cannot assume that anyone in your organization is not a risk," says Littmann. "The first time I sent a phishing email campaign out in my organization, to test our risk, the results shocked both me and our executive team in terms of the gap in our security awareness and education. It became an area of emphasis for us."

Mehring concurs. "Your largest surface area is your people component. They are the ones interacting with the Internet. They are interacting with the email services. They are interacting with things in many different ways," he says. "And so you have to accept that there's going to be a certain amount of risk there and try to do what you can to manage it."

"One thing we do after we do a phishing campaign, is reach out to the people who have been phished and direct them to education, no matter who they are or where they happen to work..." – *Stephen Nardone*

Curran says that even highly educated people can fall for phishing links. "This isn't meant to bash people because we have a lot of very smart, highly capable employees. They want to do a good job. Doctors and nurses are doing what they can to make the patient well. They are getting hundreds of emails a day. The business guys are just as busy. It can be hard to know when you are being phished," he says. "If you get an email from the Chief Financial Officer that says invoice, and it's marked urgent, there's a good chance you are going to click on that attachment."

This is why Nardone says that transparency, education, and people management are key components of any effective security strategy. Information security can no longer be delegated to a cubicle in the back of the IT department—something that only occurs behind the scenes. Any effective policy needs to touch on every aspect of the enterprise. Littmann agrees wholeheartedly.

"One thing we do after we do a phishing campaign, is reach out to the people who have been phished and direct them to education, no matter who they are or where they happen to work," he says. "This gives us an opportunity to show people just how sophisticated some of these attacks are and how to avoid them in the future."

Tools for Putting the Right Plan in Place

With such complex systems and large surface areas of penetration, how can a healthcare organization make sure it is putting the right security policies in place to ensure it is prepared for inevitable attacks?

The first step, Littmann says, is getting all your key stakeholders on board. He says that any successful cybersecurity program is going to be a collaborative one. "Getting your leadership organization on board is important. It can help you create a security education campaign across the enterprise, for starters," he says. "But it also helps you make sure that your information security organization is aligned with your infrastructure organization. Those organizations can't operate in silos, they have to operate hand in hand for a successful plan to take shape."

From there, Curran advises organizations to look at the HITRUST Common Security Framework (CSF).[xx]

"This is a great starting point to use for your gap analysis," he says. "It was designed for your compliance and HIPAA requirements. And it's the best place to begin to make sure you're covered."

Mehring suggests a look at the National Institute of Standards and Technology (NIST) Cybersecurity Framework for guidance as well.[xxi] He says NIST has some pretty easy to-do lists to help you set up a good basic security program.

"You put a plan in place for the most basic things—to start, the blocking and tackling of bad things that happen on any network every single day. You pay attention to the basics," says Mehring. "Make sure you have a plan in place to keep your systems up to date and patched. Address any gaps and figure out how you can compensate. Make sure that access is done correctly. Know where your assets are, where your data resides, and how people can get to it. Get granular enough in your plan that you know what you need to do immediately, that you don't have to search people out. You start small and build up from there."

But the plan, of course, is only as good as it is practiced and tested. Littmann tests the limits of his security programs and policies on a regular basis. "We conduct phishing campaigns. We regularly validate password strength through ethical hacking. We used these results to support increasing the complexity of our password policy, adding a dictionary filter. We leave USB sticks lying around and see if anyone picks it up and puts it in a drive," he says. "We do some social engineering. We run penetration testing and risk assessments on a regular basis. We test our policies and make sure they are holding up. And we often work with third-party vendors to do that."

Keys to Defending Against the Next Generation of Threats:

1. Getting your key stakeholders and executive leadership on board.
2. Assess and understand where your key data and PHI is housed. Assess quality of backup data and storage protocols.
3. Refer to top security frameworks from key sources such as the HITRUST Common Security Framework and NIST Cybersecurity Framework.
4. Start small with the most basic instances that can happen on the network regularly, and expand your strategies out from that point.
5. Create an automation workflow for continuous patching and updating of software.
6. Assemble a group of multi-disciplinary team members to assess different aspects of the security protocol for other departments.
7. Leverage security software and built-in hardware through servers to scan and monitor the network and manage risks.
8. Create a follow up program to continuously test and monitor penetrations into the network.
9. Install a security education plan for employees and staff, especially to combat social engineering and spear phishing.
10. Commit to regular and continuous security testing scenarios for staff and executive leadership

But Nardone says that, with such a complex infrastructure, it can be difficult for organizations to really understand their true cybersecurity risks without some outside help.

"Many organizations don't have the tools, the approach, or the skills to be able to do a good security analysis. They can't tell you whether their infrastructure does a good job of protecting them against exploitation," he says. "So it pays to look for skilled resources who are qualified to see the big picture, to understand the issues involved with mobility and medical devices, and help you manage your risk from an end to end perspective."

But it is clear that having a comprehensive plan in place is the key to an effective response. Littmann says that the security program at the Kelsey-Seybold Clinic helped them quickly identify a ransomware situation before it did any significant damage.

"We were able to identify the problem within an hour, stop the machines that were propagating the infection and limit the exposure," he says. "We did end up with close to 80,000 files that were ransomed on some file shares but were able to recover each and every one because we had a back-up approach plan in place. We were also able to identify any file that anyone touched that day and made edits to secure the last competent back-up. All in all, we had a very rapid incident response, almost no downtime, and no consideration of paying a ransom."

Curran says they had a similar situation at Cooper University Healthcare last year. "When we had our ransomware attack, we were able to quickly respond. We followed our incidence response plan and it paid off," he says. "We only had 14 PCs infected—and that's why it didn't make the news. You've got to have a plan. You've got to follow the plan. It really does make all the difference."

The costs of healthcare data breaches are staggering.

Experts agree that it's not a matter of if, but when, your organization will face a cyberattack. And the attacks are only growing in sophistication. But even healthcare organizations, with their unique infrastructures and large surface penetration areas, can be ready for any eventuality with the right kind of preparation. By working across the enterprise to create and maintain a thoughtful, comprehensive cybersecurity program, your organization can significantly reduce the risks of an expensive data breach or next-generation cyberattack, ensuring that patient health information is protected and the quality of care is never compromised.

REFERENCES

[i] HHS Press Office. 2014. "Data Breach Results in $4.8 Million HIPAA Settlements." U.S. Department of Health and Human Services, May 7. http://www.hhs.gov/about/news/2014/05/07/data-breach-results-48-million-hipaa-settlements.html

[ii] Office for Civil Rights. (n.d.). "Civil Money Penalty." Compliance Enforcement. U.S. Department of Health and Human Services. http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/examples/cignet-health/

[iii] Office for Civil Rights. (n.d.). "HHS Settles HIPAA Case with BCBST for $1.5 Million." Compliance Enforcement. U.S. Department of Health and Human Services. http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/examples/BCBST/index.html

[iv] Silva, Chris. 2012. "Blue Cross Tenn. Pays $1.5 Million for HIPAA Violation." *Nashville Business Journal*, March 13. http://www.bizjournals.com/nashville/news/2012/03/13/blue-cross-tenn-pays-15-million-for.html

[v] Green, Max. 2015. "15 of the Biggest Data Breach Settlements and HIPAA Fines." Becker's Health IT and CIO Review, October 14. http://www.beckershospitalreview.com/healthcare-information-technology/15-of-the-biggest-data-breach-settlements-hipaa-fines.html

[vi] Ponemon Institute. 2013. "2013 Cost of Data Breach Study: Global Analysis." Ponemon Institute Research Report, May. http://www.ponemon.org/local/upload/file/2013%20Report%20GLOBAL%20CODB%20FINAL%205-2.pdf

[vii] Silva, Chris. 2012. "Blue Cross Tenn. Pays $1.5 Million for HIPAA Violation." *Nashville Business Journal*, March 13. http://www.bizjournals.com/nashville/news/2012/03/13/blue-cross-tenn-pays-15-million-for.html

[viii] Health Information Trust Alliance (HITRUST). 2014. "Healthcare's Model Approach to Critical Infrastructure Cybersecurity." June. https://hitrustalliance.net/content/uploads/2015/09/ImplementingNISTCybersecurityWhitepaper.pdf

[ix] Sullivan, Tom. 2016. "More Than Half of Hospitals Hit with Ransomware in Last 12 Months." Healthcare IT News, April 7. http://www.healthcareitnews.com/news/more-half-hospitals-hit-ransomware-last-12-months

[x] Zetter, Kim. 2016. "Why Hospitals Are the Perfect Targets for Ransomware." *Wired*, March 30. https://www.wired.com/2016/03/ransomware-why-hospitals-are-the-perfect-targets/

[xi] Ferrillo, Paul. 2016. "Using the NIST Cybersecurity Framework to Combat Ransomware Attempts." *Tripwire*. January 26, 2016. http://www.tripwire.com/state-of-security/security-data-protection/using-the-nist-cybersecurity-framework-to-combat-ransomware-attempts/

[xii] Ragan, Steve. 2016. "A Blue Team's Reference Guide to Dealing with Ransomware." CSO, March 22 2016. http://www.csoonline.com/article/3046586/technology-business/a-blue-teams-reference-guide-to-dealing-with-ransomware.html

[xiii] "Investigation Launched into Main Line Health Spear Phishing Attack." HIPAA Journal, March 3 2016. http://www.hipaajournal.com/main-life-health-spear-phishing-attack-3340/

[xivi] Bowman, Dan. 2016. "Security Experts Worry About 'Spear Phishing' in Wake of CareFirst Breach." Fierce Healthcare, May 21 2015. http://www.fiercehealthcare.com/it/security-experts-worry-about-spear-phishing-wake-carefirst-breach

[xv] Tracy, Miles; Jansen, Wayne; Scarfone, Karen; Butterfield, Jason. 2007. "Guidelines on Electronic Mail Security." National Institute of Standards and Technology. http://csrc.nist.gov/publications/nistpubs/800-45-version2/SP800-45v2.pdf

[xvi] Kessem, Limor. 2015. "Shifu:'Masterful' New Banking Trojan Is Attacking 14 Japanese Banks." IBM X-Force Security Intelligence. August 31, 2015. https://securityintelligence.com/shifu-masterful-new-banking-trojan-is-attacking-14-japanese-banks/

[xvii] Finkle, Jim. 2014. "Exclusive: FBI Warns Healthcare Sector Vulnerable to Cyber Attacks." Reuters, April 23. http://www.reuters.com/article/us-cybersecurity-healthcare-fbi-exclusiv-idUSBREA3M1Q920140423

[xviii] Trend Labs APT Research Team. 2012. "Spear-Phishing Email: Most Favored APT Attack Bait." Trend Micro Incorporated Research Paper. http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-spear-phishing-email-most-favored-apt-attack-bait.pdf

[xix] Verizon Enterprise. 2016. "Understand What You're Up Against: Cybersecurity's Most Comprehensive Investigations Report Is Back." Verizon's 2016 Data Breach Investigations Report. http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/

[xx] Health Information Trust Alliance (HITRUST). (n.d.). "HITRUST CSF." https://hitrustalliance.net/hitrust-csf/

[xxi] National Institute of Standards and Technology (NIST). 2016. "Cybersecurity Framework." U.S. Department of Commerce, June 9. http://www.nist.gov/cyberframework/