UNDER SIEGE: ACHIEVING CYBER-RESILIENCY IN AN EVOLVING HEALTHCARE LANDSCAPE

healthcare informatics
CUSTOM MEDIA

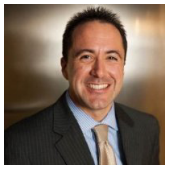
PROVIDED BY

imprivata®

Contributing Executives

Theresa Meadows, MS, RN, CHCIO, FHIMSS
CIO, Senior Vice President
Cook Children's Health System
Co-Chair, HHS Health Care Industry Cybersecurity Task Force

David Ting
Founder and Chief Technical Officer (CTO)
Imprivata



Aaron Miri
Chief Information Officer (CIO), Vice President of Government Relations
Imprivata

Introduction

Is your healthcare organization resilient enough to handle an impending cyber-attack?

Most cybersecurity experts agree: when it comes to cyber intrusions, it's not a matter of if hackers will attempt to gain entry to your network and information technology (IT) infrastructure, but when. And healthcare organizations are markedly vulnerable to these attacks.[1] The latest headlines are evidence that the when those experts speak of is likely coming sooner rather than later.

In May 2017, the United States Federal Bureau of Investigation (FBI) issued a specific warning to the healthcare industry regarding its particular—and grave—susceptibility to cyberattacks.[2] The warning, in response to the WannaCry ransomware attack that brought healthcare firms in the United Kingdom and Europe to their proverbial knees, stated, "The healthcare industry is not as resilient to cyber intrusions compared to the financial and retail sectors, therefore the possibility of increased cyber intrusions is likely."

The FBI was remarkably prescient: Within four weeks, healthcare and related organizations in the United States, including pharmaceutical giant Merck, were fending off their own debilitating cyber intrusions.[3] Organizations with strong cybersecurity strategies in place were able to prevent network invasions—or, at the very least, quickly recover from any breaches. But those organizations that were not "cyber-resilient" are likely still determining the extent of the damage.

Such damage can be astonishingly costly. The Ponemon Institute's Industry-Wide 2017 Cost of Data Breach report found that the average cost of such a breach had amounted to $225 per compromised record, due to system down times as well as recovery and restitution costs.[4] But that dollar amount per record may be even higher for medical data breaches, where organizations who cannot adequately protect patient data may face significant fines from the federal government as well as lost community and patient trust as their names are plastered on the Health and Human Services (HHS) Office of Civil Rights "Wall of Shame" breach report webpage.[5,6]

David Ting, Founder and Chief Technical Officer (CTO) at Imprivata and also an active member of the HHS Health Care Industry Cybersecurity Task Force, says that hackers are naturally drawn to healthcare because there's great value in healthcare data. "If a credit card has been compromised, the bank can put a stop on the card. The value is gone. But you can't do that with a medical record. The shelf life is much, much longer," he says. "You can use someone's medical history for influence, for blackmail, for extortion—you can find enough information in most medical records to commit identity fraud or to even get prescription drugs. But, honestly, all the ways these kinds of records could be possibly exploited is still unknown."

Black market trading of personal healthcare records is only the tip of the iceberg. Ting adds that now, with malware and ransomware attacks, cyber criminals don't have to just rely on finding ways to monetize medical records to gain from their hacks. They can take over networks and then hold individual healthcare organizations hostage for ransom instead.

"They can get in and then hold up the critical infrastructure. They can tell a healthcare organization, 'Hey, your medical records can't be used. Your MRI or other key medical devices can't be used. You won't have access to your Internet.' They now have ways to block the organization from being able to generate revenue—and will keep those organizations down until they pay," he says.

Theresa Meadows, CIO and Senior Vice President of Cook Children's Health System and the co-chair of the HHS Healthcare Industry Cybersecurity Task Force, says that many healthcare organizations also house research centers as well as research & development centers, which leave them open to attacks to further corporate espionage endeavors. "There are just so many components in healthcare that don't exist in other industries," she says. "It makes for unique threats from institution to institution."

These unique facets are why it's so important for healthcare organizations, of any size, to start making cybersecurity and cyber-resilience a key part of their IT missions, says Aaron Miri, Chief Information Officer (CIO) and Vice President of Government Relations at Imprivata.

"Healthcare organizations need to adopt the right mindset. They need to understand that healthcare is a critical industry that is under attack. I like to say that there are two types of organizations: those who have been hacked and those who don't know they've been hacked," he says. "To date, healthcare organizations always seem to be catching up when it comes to cybersecurity. They can't afford to play catch-up anymore. They need to start thinking about ways they can get farther ahead—because the hackers are only getting more sophisticated."

"There are two types of organizations: those who have been hacked and those who don't know they've been hacked."

— *Aaron Miri*

The State of Cybersecurity in Healthcare

Traditionally, the healthcare sector is viewed by technology experts as particularly vulnerable to cyber-attacks. Of all critical IT infrastructures, healthcare has the dubious honor of being one of the industries most targeted by hackers—and least prepared to respond to their intrusion attempts.[7] Ting says one reason that healthcare may be seen as behind other industry sectors is because they haven't been online as long—and, as such, have not had as much time to consider their cyber security strategies.

"If you look at energy, finance, transportation, and other industries, they made their digital transformations much, much earlier than healthcare. Healthcare went from being mostly paper-based to electronic medical records within the last seven years or so when the federal government injected billions to incentivize healthcare organizations to go digital," he explains. "The moment healthcare converted those records from paper to electronic, we made it easier for hackers to infiltrate those systems. And many organizations simply weren't ready to deal with that threat when we did so."

Meadows agrees that the healthcare sector is behind—and says that many organizations would like to find ways to be more secure, but are struggling to find a path forward.

"Healthcare is a complex industry. There are so many points of entry and so many subsectors. A hospital will have different security challenges than a physician's office. That physician's office will have different needs than a device manufacturer," she says. "These differences make it really hard to have a set of universal security guidelines that everyone can follow—everyone will have different parameters that they'll need to follow."

That lack of direct guidance—as well as the ever-changing regulatory requirements that take up so much of an individual's organization IT resources on a day-to-day basis—mean that healthcare organizations are at a disadvantage when it comes to building cyber-resiliency.

> "Healthcare went from being mostly paper-based to electronic medical records within the last seven years or so when the federal government injected billions to incentivize healthcare organizations to go digital."

— *David Ting*

To date, many healthcare IT shops have placed the bulk of their IT resources into managing the regulations put forth by the Health Insurance Portability and Accountability (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Acts. Meadows say that many organizations believe they are meeting cybersecurity mandates by making sure they are HIPAA and HITECH compliant—yet, that's just one piece of the bigger security puzzle.

"Cybersecurity is much more than what we do to protect the privacy of our patients' information," she says. "And with so much focus on patient privacy, we're far away from having a single industry standard that could regulate or give people a single roadmap of what they need to do in order to become more secure."

Ting agrees. "HIPAA does nothing to ensure that the entire infrastructure will be secure from prying eyes and prying hands. Smaller hospitals are still trying to figure out how to find the resources to meet HIPAA requirements and meaningful use," he says. "And that can get in the way of their ability to respond to the different cyber threats that you see today."

That's not to say that HIPAA is not an important component of a cybersecurity plan. Miri argues that patient privacy remains of the utmost importance in healthcare, but he agrees that hospitals and other healthcare organizations need to think beyond HIPAA in order to make sure they are ready for today's phishing, ransomware, and other cyber invasions—and the newer, more sophisticated cyber threats that are on the horizon.

"Unfortunately, there's no one-size-fits-all plan when it comes to making your organization more secure. There's no one technology that will solve all your problems," he says. "You need to understand your organization's specific needs and risks—and then layer in multiple facets of technology, process, people, and education to put a plan in place that will help you mitigate your risks. And that is something that takes time and focus."

"With so much focus on patient privacy, we're far away from having a single industry standard that could regulate or give people a single roadmap of what they need to do in order to become more secure."

— *Theresa Meadows*

The Six Key Imperatives

The Cybersecurity Act of 2015 mandated the creation of a cybersecurity task force to help determine a path forward for the healthcare industry—and help address how to best deal with cybersecurity threats in the sector.[8] Meadows is the co-chair of the Cybersecurity Task Force charged with identifying the myriad issues holding back the industry as it relates to cybersecurity—as well as providing guidance on how to better build cyber-resiliency regardless of an organization's size, scope, or specific mission. The Task Force published the Report on Improving Cybersecurity in the Health Care Industry in June 2017, relaying that the lack of staffing, funds, and frameworks is currently limiting healthcare's ability to best respond to cyberattacks.[9] They also shared six key imperatives to help healthcare organizations push for a strategic, unified plan to protect themselves from future threats:

1. To define and streamline leadership, governance, and expectations for health care industry cybersecurity
2. To increase the security and resilience of medical devices and health IT
3. To develop the health care workforce capacity necessary to prioritize and ensure cybersecurity awareness and technical capabilities
4. To increase health care industry readiness through improved cybersecurity awareness and education
5. To identify mechanisms to protect R&D efforts and intellectual property from attacks or exposure
6. To improve information sharing of industry threats, risks, and mitigations

While all of these imperatives are crucial to cyber-resiliency, when asked which may be the most important to healthcare organizations, Meadows is deliberate in her response.

"That education and awareness piece is just so important. The reality is, when it comes to security, everyone needs to be educated. We can't just leave it to the IT team or the Chief Information Security Officer (CISO)—because so many threats come through your employees or other people in your organization who don't understand the risks involved with clicking that link or not using that kind of personal device," she says. "We need across-the-board education to help people understand all the risks involved with cybersecurity so we have a chance of being able to mitigate them and deliver a security strategy that has a chance of doing what it's supposed to be doing."

Putting a Plan in Place

Certainly, with an evolving healthcare regulatory landscape as well as evolving cybersecurity threats, it can be difficult to know where to begin in order to put that strong cyber-resiliency plan in place. Yet, Ting suggests that it can start with the understanding that no plan will be completely foolproof.

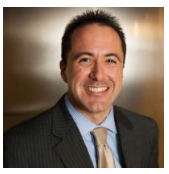
"As soon as you think you know what the threats are, the threats change. It's the nature of cybersecurity," he says. "That's why the emphasis should be on being resilient versus, 'How do I build an airtight system that can never be compromised?' You need to be able to acknowledge that you can't build a defense so that nothing bad happens—because, no matter what you do, some bad things will happen. So you need to identify the threats, find ways to detect when bad things are happening in your infrastructure, and then figure out how you can best recover from them."

Step two, Meadows reasons, should be a thorough risk assessment. "It's a real problem that so many people don't even have a baseline. They don't know what could happen—where they may be at risk from a security standpoint," she says. "If more organizations spent some time evaluating what those risks may be and putting a plan in place, even if it is just mitigation plans on how to address certain risks, healthcare, as an industry, would be a lot further along when it comes to cybersecurity today."

Miri agrees. He says that too many organizations make investments in cybersecurity solutions without having done that initial assessment—and as such, they may be ill-placed and not helping the overall cybersecurity mission.

"Before you invest anything, you need to understand where you are on the spectrum. You need to do a thorough analysis of all of your systems, top to bottom, and identify those weak links. You need to look at access. You need to look at people and education," he says. "Without doing all that, you can't figure out how to best protect yourself—or even where those investments really need to go."

"You need to do a thorough analysis of all of your systems, top to bottom, and identify those weak links. You need to look at access. You need to look at people and education."



— *Aaron Miri*

With limited IT resources, and differing IT priorities, how can healthcare organizations make sure they are placing their cybersecurity investments most judiciously—and ensure they are working towards building the kind of cyber-resiliency plan they need to thrive? The key, Ting says, is to make sure that your organization understands that cybersecurity isn't an IT issue: it's one of patient safety and care.

"Most of the CIOs and CISOs I talk to have an earnest desire to do as much as they can with the budgets that they have. They are doing their best—but the enemy is up to the task. They are equally capable of adapting to the strategies we have to counter them. It's an ongoing, escalating battle," he says. "So in order to get the resources you need, you have to change the story. It's not a story about protecting the IT infrastructure, but rather one where you say, 'Patient safety is the number one concern of this hospital. And cybersecurity is part of establishing quality care for our patients.' Because if you can't trust your infrastructure, ensuring the security of all of your medical information, your orders, and your medical devices, you put your hospital, and your patients, at risk."

> Meadows concurs. "Cybersecurity is not an IT problem. IT, obviously, has to be involved. But this can't just stay in your IT shop," she says. "Because, when it comes down to it, cybersecurity really is a patient issue. It's a strategic function of being able to provide high quality care to your patients. It may not have been historically viewed this way but that needs to change. Because if we aren't protecting our infrastructure, if we can't get the data we need or make sure the devices we use are safe, it could shut down a hospital. It could hurt, or even worst-case scenario, kill a patient. So we need to change the way we talk about cybersecurity so it can become part of the patient safety mission."

A key finding of the HHS report was that cybersecurity in healthcare is about patient safety, and for that to improve, industry stakeholders must be involved in ensuring cyber-resiliency – not just focusing on privacy. Now, more than ever, the onus is on healthcare organizations to secure their systems, medical devices, and patient data. This new emphasis on resiliency is what will allow healthcare systems to continue to operate and provide care despite increased attacks from threat actors – and it will help healthcare grow out of the "teenage years" to which Miri refers.

"Healthcare, when it comes to cybersecurity, is evolving," Miri states "I equate the industry now to the teenage years. It's kind of awkward, gangly—your arms are a little longer than your legs and you maybe have a few more pimples you don't want—but we're growing up. But with us all working together, looking at our true risks and vulnerabilities, we're going to find the way forward and finally grow up."

To learn more about cybersecurity and cyber-resiliency awareness, as well as gain insights into how to best position your healthcare organization to prevent and respond to cyber threats, visit Imprivata at https://www.imprivata.com/cyber-security-insights.

Additional Sources

1 https://www.wired.com/2016/03/ransomware-why-hospitals-are-the-perfect-targets/

2 https://asprtracie.hhs.gov/documents/hhs-update-4-international-cyber-threat-to-healthcare-orgs.pdf

3 https://www.washingtonpost.com/news/the-switch/wp/2017/06/27/pharmaceutical-giant-rocked-by-ransomware-attack/

4 https://www.ibm.com/security/data-breach/

5 https://www.forbes.com/sites/mariyayao/2017/04/14/your-electronic-medical-records-can-be-worth-1000-to-hackers/#3becb21150cf

6 https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

7 https://www.wired.com/2016/03/ransomware-why-hospitals-are-the-perfect-targets/

8 https://www.congress.gov/bill/114th-congress/senate-bill/754

9 https://www.phe.gov/Preparedness/planning/CyberTF/Documents/report2017.pdf