Better Cybersecurity through Cross-Sector Best Practices

Are the threats and risks in healthcare unique? Take a look outside of the industry.

Healthcare IT professionals accustomed to turning to colleagues to understand the latest cyber threats and defenses might want to widen that net to include peers in other sectors.

"There are general enterprise things that exist across all customers. If you run a Windows workstation or Mac OS laptops or servers, guess what? Everyone that has those same resources has the same kinds of challenges," said Steve Akers, a military veteran who now serves as both Chief Information Security Officer and Chief Technology Officer for Clearwater Managed Security Services. "It's the impact of some of those things that ends up being unique."

Akers' observation came during a webinar, *What Can Healthcare Organizations Learn from Other Industries About Cybersecurity?*, sponsored by Lenovo and Intel®. He and Andrew Lamkin, Security Architect at Intel, discussed advantages of cross-sector information sharing and outlined best practices for healthcare IT professionals to consider.

The bullseye keeps getting bigger

One reason healthcare IT professionals tend to seek advice from each other is because of the unique ecosystems they manage, which continue to grow in complexity, and the volumes of highly desired data they protect, which continue to expand daily.

"The amount that professionals in this industry have to manage, and the diversity of operating systems, software loads, actual physical layout of machines — it's just incredible," said Lamkin, who has previously worked in the aerospace and defense industries.

Other industries are also broadening digital offerings dependent on a modern IT infrastructure. However, the *impact* of a breach sets healthcare apart. For healthcare institutions, a cyberattack represents much more than an inconvenience and a potential fine; it can be detrimental to patients' health.

Threat actors know this and continue to extort healthcare organizations through ransomware attacks, knowing a hospital is more likely to pay because of what's at stake. Ransomware gangs are also aware that healthcare organizations typically have fewer IT security resources that could help ward off an attack or resolve it quickly.

> *The amount that professionals in this industry have to manage, and the diversity of operating systems, software loads, actual physical layout of machines — it's just incredible."*
>
> **ANDREW LAMKIN** | Security Architect | Intel

Applying more security controls where possible

One area where healthcare IT professionals can learn from other industries is in handling the risk posed by vendors, contractors and other third parties whose own cybersecurity practices can lead to a breach.

Both Akers and Lamkin recommend that organizations properly vet business partners' cybersecurity, not just their own. Do these potential partners have adequate security controls around their goods and services? Do they follow federal cybersecurity guidelines from organizations like the Cybersecurity and Infrastructure Security Agency (CISA) and the National Institute of Standards and Technology (NIST)? Do they adhere to the organization's own cyber policies? And do software providers bake cybersecurity into their products, or simply bolt it on at the end of the development cycle?

"Those are things that should be written into every procurement protocol," Lamkin said. "Having something written into the relationship with an established vendor is a fantastic way to use your own power to make this a little bit better."

One example of such power in reverse is the payment card industry's creation of data security standards, better known as PCI DSS (Payment Card Industry Data Security Standard), which forced merchants who accepted credit cards to comply with these new rules. That included healthcare payers and all providers who handled such financial transactions.

PCI DSS pushed laggards to update their technology and to adopt more stringent practices to continue accepting Visa, Mastercard and other popular payment cards.

"It forced an entire industry to change how it dealt with that kind of data," Akers said. "It's brought a lot of change — technically, operationally and procedurally."

Another industry that recently increased its vendor accountability is defense, which several years ago established a cybersecurity maturity model certification (CMMC) that is now required for all companies awarded Department of Defense contracts.

"That's a very powerful stick," Akers said.

Adversarial attacks span all industries

Malware, such as ransomware, frequently targets healthcare organizations. But other sectors must also stave off attacks from adversaries eager to break in, steal data and extort victims with threats of data exposure or highly disruptive IT lockdowns. Both Akers and Lamkin point to some ways industries can fortify their defenses against such attacks.

Platforms vs. perimeter: Security software is moving from traditional perimeter security to a platform approach, in part to tear down the silos and sprawl that make IT security management more difficult. Instead of responding to alerts from multiple security tools protecting different end points, security platforms do much of the monitoring, scanning and remediating vulnerabilities before cybercriminals can exploit them. This also improves visibility by displaying all network activity in one dashboard.

Red teaming: Security controls should be tested through *red teaming*, in which an in-house or hired team poses as an adversary and tries to break in. A *blue team* is tasked with keeping them out. By working together, IT professionals can discover their networks' weak spots or validate their current controls.

Endpoint defense and response (EDR): Healthcare organizations aren't the only ones worried about securing endpoints, which can be entry points for a breach. One solution is EDR software,

> *It [PCI DSS] forced an entire industry to change how it dealt with that kind of data. It's brought a lot of change — technically, operationally and procedurally."*
>
> **STEVE AKERS**
>
> Chief Information Security Officer and Chief Technology Officer
> Clearwater Managed Security Services

> “You are not alone out there. Your peers and people in different roles in different industries — they can help you build a filter on what works and what doesn’t.”
>
> **ANDREW LAMKIN** | Security Architect | Intel

which gained popularity during the pandemic for supporting remote work and telehealth.

Threat intelligence: Every security professional, regardless of industry, should keep abreast of the latest threats by subscribing to feeds from credible sources. These sources may be vendors specializing in cybersecurity or threat feeds from a government agency like CISA or the FBI. Information can also be shared through Information Sharing and Analysis Centers (ISACs), including one for healthcare that both presenters found useful.

These feeds can overwhelm inboxes with notifications, but both Akers and Lamkin recommend taking time to sift through them — especially those sent by critical vendors like those running your operating system and electronic health records (EHRs) — to determine which alerts need immediate attention.

Non-healthcare CISOs: More healthcare organizations are hiring CISOs from other industries to bring a fresh perspective to what is happening around the world in cybersecurity. Healthcare, Lamkin and Akers said, stands to gain from hard-won experience here.

More emphasis on healthcare threats

CISA is among agencies raising awareness through campaigns like its Shields Up that provides resources and recommendations to defend attacks against critical infrastructure, including hospitals and healthcare providers often caught in a cyber gang’s crosshairs.

CISA is among the sources Lamkin recommends, though both he and Akers admit there can be a high noise-to-signal ratio if IT professionals curate too many general sources. The Department of Health and Human Service’s Health Industry Cybersecurity Practices program is another resource that develops consensus-based best practices for the healthcare and public health sectors.

‘You’re not alone out there’

Healthcare IT security teams need resources that can keep pace with their digital transformations. But in an industry where patient care always comes first, these teams may need to get creative. Luckily, this where experts across industries are ready to share.

“You are not alone out there,” Lamkin said. “Your peers and people in different roles in different industries — they can help you build a filter on what works and what doesn’t. I have yet to see a case where people in different industries aren’t willing to share their experiences and what they do in practice day to day.”

To learn more about Lenovo and Intel® healthcare solutions, visit

techtoday.lenovo.com/us/en/solutions/healthcare

About Lenovo

Lenovo Health is powering the future of healthcare and life sciences technology to transform the experiences of patients who receive care, and the providers who deliver it. From server and storage infrastructure to computing, software, and solutions, Lenovo offerings help modernize clinical workflows and provide meaningful outcomes.

Innovation is at the heart of healthcare, and Lenovo Health solutions are ready to help IT teams modernize and scale for the future including AI readiness. In the evolving security landscape, we know the future of healthcare is only as good as the strength and reliability of the technology behind it, and our solutions are poised with security and data integrity in mind. Lenovo is at the forefront of healthcare & life sciences, with over 3,000 healthcare organizations using our technology solutions worldwide. We stand with IT professionals, clinicians, medical scientists and hospital administrators to share a common goal: to improve the care and wellbeing of patients everywhere.

About Intel

At Intel, our decades-long history in healthcare and life sciences has given us deep insights into the needs of clinicians, researchers, and patients. We use this knowledge in combination with our expertise in AI, ubiquitous computing, pervasive connectivity, and edge-to-cloud capabilities to create technologies that help organizations overcome complex challenges and use data in more intelligent and effective ways.

With a vast hardware and software portfolio that supports a robust partner ecosystem, we’re powering the convergence of digital technologies into instruments, devices, and tools that can improve patient outcomes and experiences, accelerate scientific discoveries, and streamline clinical and lab workflows for providers and researchers. Intel® technology delivers the platform ubiquity and the performance, flexibility, and scalability needed to transform health and life sciences and help improve the life of every person on the planet.

Produced by HIMSS®