A THOUGHT LEADERSHIP ROUNDTABLE

Beyond the Perimeter: Redefining Healthcare Cybersecurity Strategies in an Interconnected World

CHIME DIGITAL HEALTH LEADERS

imprivata®

CHIME President and CEO Russell Branzell moderated the roundtable. Contributing to the discussion were Imprivata representatives Fran Rosch, President and Chief Executive Officer, and Sean Kelly, MD, Chief Medical Officer, SVP Customer Strategy.

CHIME members participating were:

Timothy Calahan
Chief Technology Officer
Michigan Medicine

Glynis Cowart
Vice President & Chief Information Officer
Montefiore St. Luke's Cornwall

Jeff DeFord
Vice President & Chief Technology Officer
Parkland Health

David Finkelstein
Chief Information Officer
RiverSpring Living

Mark Combs
Chief Technology Officer
Vandalia Health

Deborah Inouye
Director of Technology & Project Management
Palomar Health

Deborah Muro
Chief Information Officer
El Camino Hospital

INTRODUCTION

Imprivata convened a thought leadership roundtable with members of the College of Healthcare Information Management Executives (CHIME) to discuss how healthcare leaders can develop more effective cybersecurity strategies in the wake of increased cyberattacks, global outages, and an ever-expanding attack surface. Health system leaders identified the top challenges they face, explored some of the steps they've taken in response, and outlined the role of artificial intelligence (AI) and other technology in protecting their organization against sophisticated threats and hidden vulnerabilities.

SUMMARY

Providing high-quality patient care may be the top mission for healthcare executives, but when it comes to the biggest priority, CHIME's forthcoming Digital Health Most Wired 2024 survey found improving cybersecurity tops the list. Given the endless stream of ransomware attacks against health systems, as well as the long-term impacts of outages that hit third-party service providers such as Change Healthcare or CrowdStrike, it's hard not to see why.

"Patient care is still the primary mission, but cybersecurity is keeping healthcare IT leaders up at night," Branzell said. "And it has become a top concern of C-suites and boardrooms."

Cybersecurity is difficult to address because health systems must keep so many balls in the air at once. They must protect against intrusion at all endpoints, even (and especially) the ones over which they have no visibility. They must constantly monitor for threats and respond in real time. They must secure systems that are both mission-critical and, due to their age, un-patchable. They must educate end users in a wide variety of roles about cybersecurity and social engineering best practices. They must maintain and update business continuity plans. The list goes on – and they must do it all with a limited budget and without disrupting patient care.

If there's a common theme among these many demands, it's that they highlight the risks of providing high-quality care in an interconnected world. Medical devices in the hospital and the home share real-time data with clinical systems. Physicians can review medical records or place orders from just about anywhere. Provider organizations are both empowered and required to exchange information with each other.

SUMMARY CONTINUED

In building a cybersecurity strategy, healthcare leaders must strike a balance between improving their existing foundation – with approaches such as zero trust, continuous monitoring, and infrastructure modernization – and looking toward the future. They see a need to respond to the challenges in front of them while advocating for advanced technology and a robust policy that places their organizations on solid cybersecurity footing so they can prioritize patient care once again.

TOP 10 CYBERSECURITY CHALLENGES

While roundtable participants acknowledged there's no shortage of obstacles to improving their cybersecurity posture, 10 challenges stood out. Critically, many of them are intertwined.

Access management. Organizations struggle to ensure individuals are only granted access to the data, applications, devices, and services they need for their unique role. "Defining user roles and implementing role-based access control is a critical component to every organization's cybersecurity strategy," advised Mark Combs, CTO, Vandalia Health. "We need to understand what everyone's supposed to be doing, who should be using what things, and who shouldn't be using what things. If a user has too much privilege and gets hacked, attackers can easily move laterally across a network."

User onboarding. The variety of individuals who need to log on further complicates access. Many are everyday users, but contractors, medical specialists, or community-based providers may use enterprise systems so infrequently that their passwords are automatically reset each time they log in. Proper validation of these identities is crucial but contributes to a fragmented workflow.

Remote access. As health systems expand their physical footprint, and as clinical care moves to remote settings, security teams increasingly see log-in attempts from unfamiliar locations. "We have to verify who someone is before we grant access to systems," said David Finkelstein, CIO, RiverSpring Living. "It's frustrating for end users, but I'd rather have it that way as opposed to leaving the door open for outsiders to get into our network."

User experience. Multi-factor authentication for identity verification or device segmentation, which separates personal and business use cases on an employee's device, are necessary steps for improving security. At the same time, they can fatigue users who are simply trying to do their job. "It is important to manage the change with users, including communication and documentation of procedures and policies, so everyone's on board with it," said Deborah Muro, CIO, El Camino Hospital.

Password management. Increased adoption of interconnected enterprise systems, such as the decision support or analytics tools that integrate with the electronic health record (EHR), leaves users with dozens of passwords to remember. This leads to poor security practices such as weak passwords, shared passwords, or passwords written on paper. It also contributes to an influx of password reset requests that bog down the Help Desk.

Attackers' use of AI. AI makes it easier for bad actors to identify high-profile user accounts within an organization, tailor attacks to their role, and mimic the colleague or vendor an employee engages with regularly. These attacks are less obvious to the naked eye. Busy or stressed-out employees – sadly all too common in a healthcare setting – are increasingly susceptible to the bait.

The limitations of user education. Many panelists cited users as the biggest cybersecurity challenge. While some issues stem from bad behavior, others result from the sophistication of threats users face. Leaders can tell users to be vigilant, but education only goes so far. "We're doing a lot of things to hit each segment of our user base, but unfortunately, there's no catch-all to solve all our problems," said Glynis Cowart, VP and CIO, Montefiore St. Luke's Cornwall.

Technical debt. It's no secret many health systems rely on mission-critical legacy applications. Leaders know these back-end systems need to be updated, but they risk breaking vital configurations if they do so. "While we're busy racing forward, we need to look in the rearview mirror and review the security templates that might have been forgotten or neglected," said Jeff DeFord, VP and CTO, Parkland Health.

> "While we're busy racing forward, we need to look in the rearview mirror and review the security templates that might have been forgotten or neglected."
>
> **Jeff DeFord**
> VP & CTO
> **Parkland Health**

Third-party management. Technical debt often extends to technology partners, many of whom have their own legacy systems in place that provide difficult to patch. "We ask vendors if they support LDAP [Lightweight Directory Access Protocol] or SAML [Security Assertion Markup Language] – which has been around since the mid-2000s – and many of them say no," DeFord said. "It's a real concern."

Executive buy-in. For all the cyberattacks that make headlines and impact both patient care and the bottom line, security and IT leaders still struggle to get other executives to understand the significance of avoiding a cybersecurity incident. Competing business objectives and limited funding certainly don't help the cause.

RESPONDING TO TODAY'S THREATS

Not surprisingly, health system leaders facing a multitude of cybersecurity threats elect to take a multifaceted approach to bolstering security. Expert panelists indicated their responses address equal parts technology, policy, and overall strategy.

MOVING BEYOND "YES OR NO" POLICIES

Healthcare has long talked about moving care delivery beyond the four walls of the hospital. While this provides a better patient experience, it also means supporting end users and applications far from the traditional corporate firewall.

Timothy Calahan, CTO at Michigan Medicine, said this means "revisualizing" existing policies for access and authorization. Much of this is based on context. "If you're on-premises, we have a certain set of credentials and a certain set of prompts," he noted. "If you're off-premises, or using a device that maybe isn't secure, there are different strategies and prompts associated with that."

MOVING BEYOND "YES OR NO" POLICIES CONTINUED

Sean Kelly, MD, Chief Medical Officer at Imprivata and a practicing emergency physician, said digital identity can play a key role here. Providing a unique identity to each end user, application, medical device, or other "machine" with access to sensitive information, and assigning role-based privileges to each identity, makes it possible to move beyond the security dichotomy of locking everything down or opening everything up.

"If you know the digital identity, you can be adaptive in your response. You can dial up and down and optimize workflows while actually making them safer and more secure at the same time."

Sean Kelly, MD
Chief Medical Officer
Imprivata

"If you know the digital identity, you can be adaptive in your response. You can dial up and down and optimize workflows while actually making them safer and more secure at the same time," Kelly said. "If I'm doing what I normally do from a place I normally do it, then that should be more easily allowed than if I'm somewhere else or there's a pattern of aberrant behavior."

BUILDING REDUNDANCY ON-PREMISES

Accompanying the shift of care delivery and resources beyond the hospital campus is the shift of applications, data, and computing resources to the cloud. This is poised to cut operating costs, improve flexibility, and provide scalability – all of which are valuable to organizations at a time when budgets are tight.

That said, the Change Healthcare and CrowdStrike outages reminded health leaders about the benefits of onsite redundancy. "We're making offline copies of critical documents in almost every single department in the event of another outage," RiverSpring Living's Finkelstein said. "It costs time and energy, but it's a necessary cost to continue operations."

Muro similarly noted that El Camino Hospital has invested in a backup dictation system after its primary provider went down several years ago. Echoing Finkelstein, Muro said it's an additional but necessary expense.

Leaders also need to consider end user support when always-on systems suddenly go down. "There's a generation that walks into our hospital now that only knows how to do things electronically," Montefiore's Cowart pointed out. Patients' needs don't change just because the EHR is offline. What backup systems need to be in place so medications can be administered and care decisions can be made?

HOLDING THIRD PARTIES TO HIGHER STANDARDS

The shift to the cloud, coupled with the adoption of third-party tools for use cases as diverse as remote monitoring, marketing, supply chain management, and data analysis, leaves health systems increasingly reliant on external partners for security. This can have benefits, particularly given the expertise and tools in place for leading cloud service providers. At the same time, health system leaders are understandably hesitant to trust things they cannot see.

HOLDING THIRD PARTIES TO HIGHER STANDARDS CONTINUED

"Are we not just shifting the risk from what you have on-premises to the third-party provider?" Finkelstein asked. "They're a giant honeypot if they get hit with a ransomware attack or stolen credentials."

One mitigation strategy is to hold partners to higher standards. It's a delicate process; requesting a patch or updating your own requirements may tip the apple cart for a relationship that has spanned decades. But leaders say it's essential for protecting employees and patients alike.

"We need to implement new ways of doing things, but they want exceptions granted. We can't do that – because if they're at risk, that puts us at risk," said Deborah Inouye, Director of Technology & Project Management, Palomar Health.

> "We need to implement new ways of doing things, but they want exceptions granted. We can't do that — because if they're at risk, that puts us at risk."
>
> **Deborah Inouye**
> Director of Technology & Project Management
> **Palomar Health**

A VISION FOR THE FUTURE OF CYBERSECURITY

Modifying access policies, building redundancies, and holding third parties accountable are important actions to take today. Looking to the future, health system leaders see promise in the further application of technology coupled with stronger action on Capitol Hill.

RiverSpring Living's Finkelstein said he'd like to see governments "clamping down on the bad actors across the world." That way, health systems are positioned to devote fewer resources to defense and more to supporting their core business. As Montefiore's Cowart put it: "We need to get back to being able to take care of our patients the way that we should without fear."

El Camino Hospital's Muro suggested the government could give organizations a nudge to improve. The Department of Health and Human Services released voluntary cybersecurity performance goals earlier this year, aiming to help health systems implement "high-impact cybersecurity practices." The next step is financial incentives similar to those in place for EHR use, care quality, and value-based care. "We need to start having those – if we don't meet them, then we don't receive a reimbursement."

On the technology front, health systems leaders see potential for broader application of AI in cybersecurity defense. Automation can be a vital tool on several fronts, from patching security vulnerabilities to identifying, analyzing, and mitigating threats to authenticating users for seamless log-in.

In fact, a passwordless future may be the answer for healthcare.

"Usernames and passwords were used at least 60 years ago, and organizations today are still using this old approach to manage access for thousands of users," Branzell noted. "The advanced technologies to go passwordless have existed for many decades — military used retinal scan 40 years ago."

According to Imprivata's Kelly, AI-enabled approaches to authentication can include facial recognition, biometrics, and Bluetooth-enabled location awareness. Done right, an identity management system will "sniff out" signs of abnormal behavior and ask for further credentials. On the other hand, if a credentialed and verified clinician walks into an exam room, the system can automatically call up the EHR – and then close it down once they walk away.

Imprivata CEO Fran Rosch said this approach enables a shift away from the "static environment" of one-size-fits-all usernames and passwords – and the numerous challenges they present.

"We think of passwords as a lose-lose situation," he said. "It's a bad experience, because who wants to create, manage and reset another username and password? It's also bad security, because people can be phished and give them away."

There's an additional benefit to modernizing authentication, Rosch added: Organizations can spend less on cybersecurity training when they're reassured that end users aren't sharing passwords or exposed to threats from malicious actors who gain easy access. "We're getting to the place where technology can allow users to just go in and do their work without needing extensive training."

CONCLUSION

It's no secret health systems face a range of cybersecurity challenges. Addressing these concerns is all about balance – keeping bad actors out while providing fast access to verified identities, adopting modern technology while security legacy systems and building on-premises redundancies, and so on. The growth of the physical and virtual hospital network beyond the traditional perimeter only makes things more complicated.

Health system leaders are doing their best to keep their organizations safe and stay out of the headlines. They're adopting policies that bring context to access and authorization and don't simply offer the keys to the kingdom. They're working closely with longtime technology partners to ensure their vulnerabilities don't translate to added risk for the health system. They're looking to eliminate common points of weakness, such as passwords, which attackers have previously been all too happy to exploit. Though no single step is enough, together they represent a cohesive strategy to strengthen cybersecurity in challenging times.