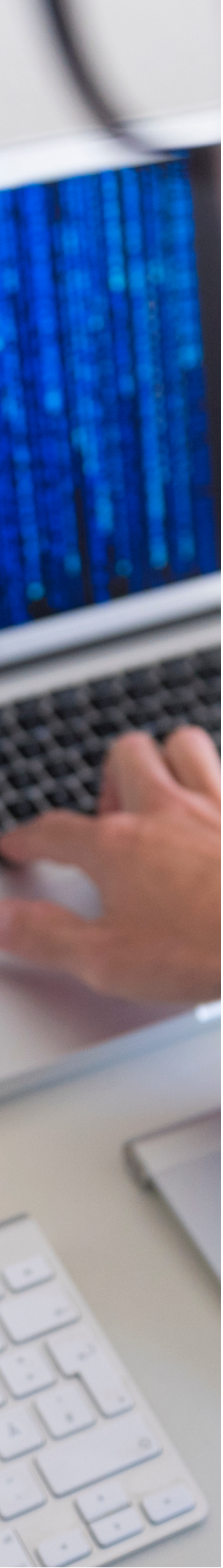
TACKLING CYBERSECURITY THREATS WITHOUT SACRIFICING USABILITY

Insights, Best Practices, and Solutions From Executive Leaders

PREPARED BY

LexisNexis® RISK SOLUTIONS | Health Care

EHI EXECUTIVES FOR HEALTH INNOVATION



On April 13, 2022, a small group of cybersecurity professionals convened for an executive roundtable, "*Tackling Cybersecurity Threats Without Sacrificing Usability*." Participants collaborated with the purpose of sharing their experiences of protecting their health system and patients from cyber-attacks while also retaining optimal user experience.

Through the COVID-19 pandemic, cybersecurity threats to hospital systems rose 123%[1] and ransomware, more specifically, affected more than 18 million patient records nationwide – a 470% increase from 2019.[2] The same report found in 2020 alone, hackers pulled in more than $2.1 million in ransom.[3] ECRI named cybersecurity attacks as the top health technology hazard to patient safety for 2022.[4] The risk to patient lives have never been higher.

Attendees at the roundtable shared solutions being developed, innovative plans being implemented, and best practices created through personal experiences. The discussions allowed the executives to shed light onto the greatest vulnerabilities to patient safety.

DISCUSSION HIGHLIGHTS

- Attacks on health systems are inevitable, it is not a matter of if, it is when. Chief information security officers and their teams across the healthcare industry are developing defensive plans and training their teams for one of the worst days of their professional lives.

- Well-meaning security plans can quickly become barriers to the access of quality care if deliberate caution by leadership is not taken. Cyberteams must carefully balance security procedures with usability features for patients.

- Cyber-attacks generally impact all critical departments within a hospital, including billing, laboratory, medical records, and personnel management. To truly prepare the health system for a cyber-attack, all members of the health system's staff should be trained to respond, defend, and recover.

- Federal regulators need to find a balance between implementing data interoperability regulation and enforcement, and allowing the healthcare industry the independence it needs to innovate.

- To the cyber-crime world, a hospital is seen as an easy target with big reward. It's the cybersecurity team's job to create a system that protects patients' data from theft and the potential deadly outcomes.

FEATURED SPEAKERS

Jackie Evans, Director, Information Security, Mayo Clinic

Greg Garneau, Chief Information Security Officer, Marshfield Clinic Health System

Jeri Koester, Chief Information Officer, Marshfield Clinic Health System

Malikah "Mikki" Smith, Chief Information Security Officer, Office of the National Coordinator for Health IT (ONC)

Jay Sultan, Vice President, Healthcare Strategy, LexisNexis Risk Solutions

Adam Zoller, Chief Information Officer, Providence Health

What is the federal government's primary focus on cybersecurity?

Mikki Smith (MS), Office of the National Coordinator for Health Information Technology: "Our primary focus is to continue to take steps to encourage the development and implementation of technology to enable healthcare providers to operationalize what we have as existing laws and policies, including those related to protecting and securing health information."

How is ONC working with the healthcare industry to protect patient data?

MS: "[ONC] wants to encourage ... privacy and security being implemented by design. One challenge is getting those things [done] at the front end and not trying to do them afterwards. And then ensuring that we're including specific controls that help to protect patient information and systems such as authentication and correct encryption.

"ONC also has the Information Sharing Rule that supports patient electronic access to their health information, including sharing health information with a third-party of a patient's choice, putting the power of the data and the patient hands. Making sure that they understand how they can ensure their information is secure. ...We want [patients] to have access to [their] information."

How does a hospital build their cybersecurity system?

Jeri Koester (JK), Marshfield Clinic Health System: "[At Marshfield Clinic], we annually look at cybersecurity [with questions like:] 'How do we continue to stay ahead?'; 'How do we look for our greatest threats and vulnerabilities'?; 'What can we continuously do to close those gaps?'

"[This discussion has] led us [to build] a list of things that we are continuously working on. A lot of things [revolve] around technology decisions: from our alerting response and threat hunting, to addresses that are ambiguous or threats.

"[My team has] started working with the business [side of MCHS] around tabletop exercises. We work with our emergency response team, and we are going into each one of the areas of the business unit in order to make sure if something did happen, they understand how they will continue to operate."

How do you build a cybersecurity system that works for your specific hospital?

Adam Zoller (AZ), Providence Health: "[I'd say] use your [health system's] culture to your advantage. At Providence, for example, our organizational culture is aligned around providing people quality care no matter what walk of life they come from. In our case, especially the poor and the vulnerable. [You should] provide [quality care] to those who wouldn't normally be able to afford it.

"The same thing [goes for our] security [system]. We bake security services into the services [we already] deliver to the patient. They might not necessarily know anything about cybersecurity, but they should walk through our doors, knowing that their data is secure and that the care we deliver to them is via a secure healthcare device, so that they don't have to worry about this stuff when they're focused on getting better."

Have any recent cyber incidents made you rethink security strategy?

JK: "[Yes,] we've always had security reviews as part of the purchasing process [for medical devices] and the reviews of the service level agreements that we have with our vendor partners, but with the Kronos event we've really started digging into that third party risk management portion of cybersecurity and understanding their downtime accessibility to the data recovery process."

Greg Garneau (GG), Marshfield Clinic Health System: "Kronos was a heck of a wakeup call for a lot of folks. [Now we ask:] 'What happens when payroll goes down two weeks before Christmas?' 'How are you going to pay your teams?' This becomes not just an exercise in cybersecurity but an exercise in business continuity planning. A main focus is cyber resiliency as it related to impactful events, not just for our organization but our vendor partners."

How do you train for a cyber-attack?

AZ: "You always want to train in the same situation…and act as if you're fighting the fight during peacetime so that when you actually have to use those skills it's not the first time that you've pulled out the manual and tried to figure things out. … A saying we had when I was in the army is 'you train like you fight'…[It] becomes muscle memory.

"The other thing is having an incident response plan (IRP) to test in tabletop exercises. As Mike Tyson said, 'Everyone has a plan until you get punched in the mouth'.

You have to have flexibility built into your plans to the point where you can just adjust as needed. Don't be so rigid in sticking to that plan. Testing that during the tabletop is the best way to do it."

It's widely recognized in the cybersecurity world that most instant response plans (IRPs) are thrown out the moment an organization is attacked. Why develop an IRP if it likely will not be used?

AZ: "The most important lesson that I've learned over the last few years is the importance of having a strategy. Strategy encompasses the organization's goals and objectives and direction and how security is used as a business enabler to drive those goals and objectives as an organization forward. It's broader than just technical or operational tasks."

What must hospitals systems think about when they are starting to develop their IRPs?

AZ: "Focus on risk and not just the threat. 'What are you doing about ransomware attacks?' Well, that's just the threat. We need to focus on threat, but that's just one calculation that feeds into the risk equation. 'What does our vulnerability posture look like?' 'What's the opportunity that we're presenting to the threat actors to take advantage of those vulnerabilities?'. And 'what does the threat landscape look like and how does that holistically speak to the risk as a system?'

"I think it's an incredibly important [to think of] cybersecurity as a risk reduction mechanism, not a threat management mechanism necessarily. [It's important to remember that] it's not about the number of incidents that we faced or overcame over the last time. 'What are the business outcomes we're trying to drive by reducing cybersecurity risk, so that we can operate more securely?' And then, lastly, [we need to think about] aligning our organization to an industry model that has [worked]."

How do you prepare executive leadership for a ransomware attack?

JK: "[The preparation] is an extensive conversation about data, and [decisions around] when you do have compromises. When it's a ransomware attack, you first have to figure out how long they've been in your system. And you don't know where the compromise is which, as we all replicate data becomes another conversation about 'is the backup anything we can use?'

"When you have a ransomware attack, [the information security team is] going to need input from our operational partners. [Ensuring everyone has an] understanding of their role and including our CEO and board's responsibility in the event that something like that happens."

How do you help executive leadership understand the importance of spending on cybersecurity?

Jackie Evans (JE), Mayo Clinic: "Money is, in many cases, a bridge to translation, but comparing cost against value is essential. We are working on defining cost per unit of service in our assessment, architecture, and resilience areas so we can quantify cost against value, in this case, the risk reduction to Mayo Clinic."

How do you help your technology team think about the budget?

JE: "We ensure our cybersecurity professionals understand our primary value and that expenses to reduce risk result in a cost to the institution, and our care providers."

AZ: "[I remind my team that] every dollar we spend on cyber comes out of the pocket of patient care."

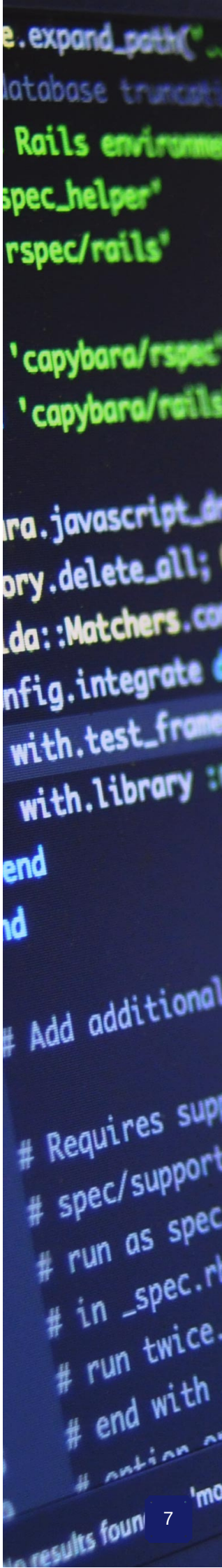
How do you balance a secure system and unencumbered patient access?

JE: "The basics are important here, and educating our patients to use protection like multi-factor authentication and using unique passwords as well as passphrases are important to protect their data."

MS: "[I think] educating the user and making it easy for them to understand is also a part of getting them to see that they can have access to their information but [that] there is some shared responsibility around making sure that they get [the information] securely and that they're able to use it securely. We also have a digital divide challenge, depending on the age group.

"I really think that literacy and consumer literacy [have become] a big part of the picture."

Jay Sultan (JS), LexisNexis Risk Solutions: "[The healthcare industry] wants to make the system super secure, but [this can lead to] unintended consequences if [the industry leaders] are doing so in a way that's not thoughtful, it may be creating barriers for some of the very people we most want to be able to access the data.



“Patient consumer topics are where we, [in the industry], have the highest need to make sure that we’re being secure, but we also have to think about the range of capabilities of the [user] and not unknowingly or unthinkingly create barriers that allow some people access but preclude access from others. I think this is particularly true when we start thinking about more digital consumer experiences and healthcare. For example, ‘I want to see my test results’, and ‘I want to download an app so that I can access telehealth’.”

How do you teach users how to build up their personal security?

JE: “I’m a big believer in ‘just-in-time’ learning. Not just for our patients and consumers, but for our physicians as well. If you put [the lesson] right at the point in time that I need it, there’s a much better chance it will be seen and used and incorporated it into day-to-day workflows.

"We are working on implementing a password ‘strength meter’, that give users guidance when choosing passwords.”

Why do users resist additional security controls for their medical records?

JE: “[The first thing to note: we] have been using multi-factor authentication to sign into [our] bank accounts for years. Many of us expect that. Providing multi-factor to a medical record may present challenges to patients who see it as a barrier to accessing their medical record, but it is a necessary measure to protect that personal information.”I think helping them understand how [the process] protects them is key.”

AZ: “At Providence, many challenges in deploying security capabilities don’t stem from leadership, but rather from the organization’s culture. This is widespread throughout the healthcare industry. People have been doing the same thing for a very long time and they don’t want to change. It’s human nature.

“[Providence health] rolled out multifactor authentication a few years back and I immediately received a huge volume of mail from mostly front-line caregivers who haven’t needed to use modern security features in their role”

Adam, how did you solve the user’s concerns?

AZ: “[I spent] time with each of those individuals to [help them] understand the seriousness of the threat that we were facing at the time. Which was active targeting by ransomware groups. And [I explained] why it was important to have multifactor authentication as a baseline minimum.”

What is the biggest lesson you learned during the pandemic?”

Mikki Smith, ONC. “We have to get over this whole fear of risk and this risk intolerance, we have to understand that we are always making a risk-based decision. And just communicating that it’s okay; it’s more important to be able to say ‘I know our risk factors are high here and this is where I want to expand my budget’.”

Jeri Koester, Marshfield Clinic. “Beg, borrow and steal from other industries that are doing well.”

Adam Zoller, Providence Health. “Take care of yourself and take time to reinforce [to the] people who work for you [that they] should be taking care of themselves as well… Cybersecurity is a very technical problem, but it’s also delivered by humans for organizations that are run by humans. It’s a very human-centric problem.”

Greg Garneau, Marshfield Clinic. “We just have to think of really crazy ways to find staff and talent in order for us to continue to provide services to protect patients.”

Jackie Evans, Mayo Clinic. “I would say don’t get too comfortable where you’re at.”

CONCLUSION

COVID-19 has stress tested hospitals like never before—pushing cybersecurity professionals to rapidly innovate their systems and thoroughly plan for the impending cyber-attack. There are very few silver linings to this global pandemic, but one may be the focus that cybersecurity is receiving from top executives in the healthcare industry. Cybersecurity professionals are communicating the problems and health organization leadership is listening and learning. It takes more than a well thought-out plan and a well-educated staff to fend off bad actors. It takes continuously innovating systems using the most up-to-date technology, implementing regulations as they arise, utilizing best practices and hiring an inventive cybersecurity workforce.

A hospital's central foundation is patient care, and cybersecurity is a piece of the entire framework that gives patients the ability to feel safe.

ENDNOTES

[1] https://www.sonicwall.com/2022-cyber-threat-report/
[2] https://www.fiercehealthcare.com/tech/ransomware-attacks-cost-healthcare-industry-21b-2020-here-s-how-many-attacks-hit-providers
[3] https://www.comparitech.com/blog/information-security/ransomware-attacks-hospitals-data/
[4] https://www.ecri.org/press/ecri-names-cybersecurity-attacks-the-top-health-technology-hazard-for-2022

About Executives for Health Innovation

Executives for Health Innovation (EHI) is a catalyst for healthcare transformation, convening diverse leaders from across the industry to unlock opportunities for collaborative innovation. EHI, along with its coalition of members, focuses on education, thought leadership, and advocacy. We believe that innovation and diverse perspectives power the transformation of healthcare. Our members are working toward consumer-centered health that is lower cost, higher quality, and more accessible for all populations. **www.ehidc.org**

EHI | EXECUTIVES FOR HEALTH INNOVATION

About LexisNexis® Risk Solutions

LexisNexis Risk Solutions harnesses the power of data and advanced analytics to provide insights that help businesses and governmental entities reduce risk and improve decisions to benefit people around the globe. We provide data and technology solutions for a wide range of industries including insurance, financial services, healthcare and government. Headquartered in metro Atlanta, Georgia, we have offices throughout the world and are part of RELX (LSE: REL/NYSE: RELX), a global provider of information-based analytics and decision tools for professional and business customers. For more information, please visit **www.risk.lexisnexis.com** and **www.relx.com**.

LexisNexis® RISK SOLUTIONS | Health Care