EXECUTIVE SUMMARY
The Scottsdale Institute virtually convened 29 Chief Information Security Officers (CISOs) from 24 member organizations for an annual Summit, sponsored and moderated by Deloitte, on December 4, 2020. Representing myriad medical centers across the U.S., these professionals came together to share their experiences and suggestions for building safe, healthy remote-working environments and educating key executive management teams on cyber risk as the nation battles COVID-19 and IT security needs skyrocket.

In discussing whether the pandemic has created a likely permanent shift in how, when and whether employees can work from home successfully, Summit participants shared their organizations’ risk-management experiences with their boards and C-suite executives, their long-term plans to shore up security and business-continuity objectives and their challenges with connecting remotely (and empathetically) to team members.

SUMMIT OBJECTIVES
» Effectively engage board and executive management in enterprise risk management
» Strengthen business-continuity management to minimize threats and impacts to resiliency and recovery from COVID, ransomware and other disruptions
» Build a risk-awareness culture in the mobile workforce and adjust “the way we’ve always done things” to better protect the organization
» Focus on workers’ mental health, peer connectivity and career development options in remote settings
SUMMIT PARTICIPANTS

Myles Angell, Director, Infrastructure & Operations, Baystate Health
Chris Convey, VP & CISO, Sharp HealthCare
Steve Crocker, CISO, Methodist Le Bonheur
Michael Czumak, VP & CISO, Memorial Sloan, Kettering Cancer Center
Erik Decker, Chief Information Security & Privacy Officer, University of Chicago Medicine
Scott Dresen, SVP & CTO/CISO, Spectrum Health
Michael Erickson, CISO, Baptist Health
Todd Greene, VP & Enterprise CISO, Atrium Health
Jim Hanson, ISO, Avera Health
Todd Hill, Director, IS & Deputy CISO, Baptist Health
Tricia Julian, CIO, Baptist Health
Jigar Kadakia, CISO & PO, Mass General Brigham
Thien Lam, VP & CISO, BayCare Health System
Lenny Levy, CISO, former Providence
Meridith McGlincy, CyberSecurity Director GRC/SM, Intermountain Healthcare
Ron Mehring, VP Technology and Security & CISO, Texas Health Resources
Helen Mohrmann, CISO, University of Texas, System
Janet Norton, Chief Legal & Regulatory Affairs Officer, Baptist Health
Shane Rodabaugh, VP, IT Infrastructure, Baptist Health
Peter Rucys, CISO, Tampa General Hospital
Sanjeev Sah, VP & CISO, Centura Health
Dean Schultz, CISO, Virginia Mason Medical Center
Pavel Slavin, VP & CISO, Froedtert & Medical College of Wisconsin
Bonnie Stith, Board Member, Baptist Health
Robert Turner, DIS, Bronson Healthcare
Paul VanAmerongen, VP, CISO, UW Health
Patrick Voon, CISO, Loma Linda University Health
Randy Yates, VP, CISO, Memorial Hermann, System Services
Larry Yob, Interim CISO, AMITA Health and DIS, Ascension

CONVENER

Scottsdale Institute: Janet Guptill, FACHE/Executive Director, Cynthia Schroers, Janice Wurz, Nancy Navarrette, Gordon Rohweder, Chuck Appleby, Shannon Conley, Genevieve Hedland-Hill, Patrick O’Hare, Courtney Olson, Margaret Shea, Shelli Williamson

SPONSOR

Deloitte

Moderators: Raj Mehta, Partner, Healthcare Cyber Risk Services; Mary Galligan, Managing Director

Writer: Karen Sjoblom
Board-Level Enterprise Risk Management

Innovating around COVID-19, protecting EMRs, developing procedures for remote workers: There’s no shortage of critical projects in healthcare IT these days. But no matter the topic, communication, structure and protection are key cornerstones upon which to build, with trust at the foundation of it all—trust from workers, for leaders and around cybersecurity guideposts.

As those in charge of architecting cyber safety, healthcare CISOs have had to become even more adept at problem-solving, delineating and amending their safety blueprints to address ever-changing and expanding threats from nefarious outsiders (and even from well-meaning insiders, thanks to COVID’s work-from-home mandates). As experts convened at a recent Scottsdale Institute Virtual Summit, hosted by Deloitte, they addressed the best ways to:

» build trust in board-level enterprise risk management,
» reinforce C-suite risk assurance/business-continuity management and
» construct a more risk-aware culture in the mobile workforce.

LAYING THE FOUNDATION

How do healthcare organizations build cyber trust at a board level? Seemingly brick by brick: Controls are evaluated and implemented for constant vigilance. Then, experts determine potential pitfalls and make informed decisions toward protecting critical assets. And key board committees and management utilize resulting cyber metrics for understanding threats and countermeasures...all for a unified, cohesive approach against threats and toward safety.

Ideally, this process would flow continually, uninterrupted, but as cyber-attacks and threats get more voluminous and serious, it begs the question: Are CISOs aligned with the questions the board and management need answered? Just like choosing the right tool for the job, it’s a matter of having the right conversations that offer alignment to meaningful risk data and provide more data-driven documentation toward clearer metrics. Boards are asking, “Are we safe?” But CISOs know there’s no
It seems there are two types of boards: One with a data/analytics focus (‘Show me proof’) and one that considers, at much larger scale, ‘What is the cyber impact to our organization?’

— Jigar Kadakia, CISO & PO, Mass General Brigham

INVITING EXPERT INSIGHT

“We’ve been on this journey many years and have learned to offer our board a clear communication pathway and structure,” said Baptist Health CISO, Michael Erickson. “I believe our board appreciates having access to external experts who can provide independent advisory and assurance services in addition to internal information about our security controls. The combination of these perspectives breeds trust and accountability.”

Toward that end, Baptist Health’s board of directors purposefully invited Bonnie Stith, President, Stith Associates Coaching and Consulting, LLC, and former Director of the CIA Center for Cyber Intelligence, to join Baptist’s board of directors. Including a cyber-savvy individual on the board offers a well-rounded, well-versed approach to comprehensive cyber governance. Bonnie offers her wisdom alongside Janet Norton, Chief Legal & Regulatory Affairs Officer.

With limited time for board member and group discussion, Erickson believes a key aspect of board engagement is providing board members with information to inform risk appetite and risk tolerance. Baptist Health established its cyber security program roles and responsibilities with that in mind, as follows.

setting intentions

1. Directors need to understand and approach cyber security as a strategic enterprise risk, not just an IT risk.
2. Directors should understand the legal implications of cyber risks as they relate to their company’s specific circumstances.
3. Boards should have adequate access to cybersecurity expertise; discussions about cyber risk management should be given adequate board meeting time regularly.
4. Directors should set the expectation that management will establish an enterprise-wide, cyber risk management framework with adequate staffing and budget.
5. Board-management cyber risk discussions should include identification and quantification of financial exposure to cyber risks and which risks to accept, mitigate or transfer (such as through insurance) as well as specific plans associated with each approach.

National Association of Corporate Directors Cyber Handbook, Feb 2020
» The **Board Audit and Enterprise Risk Committee** provides cyber program oversight and risk assurance on a quarterly basis aided by external advisory and risk assurance services.

» The **Enterprise Risk Management Committee** is an internal senior management committee that also meets at least quarterly and sets direction for cyber program initiatives and ensures the implementation and velocity of maturation align with board expectations.

» The **Cyber Security Committee** meets monthly and is responsible for operational cyber risk management decisions.

Throughout their tenure, the Baptist cyber risk team has reported program metrics and established a cyber maturity program to explain initiatives and determine priorities.

“We’ve really evolved over the past five years toward an enterprise-risk focus,” Norton explained. “As we’ve moved away from a representation-type board and grown in complexity as a large medical group, we believe governance is vitally important. We are very intentional in selecting board members for their expertise—legal, banking, cyber intelligence, insurance and the like—so we have a small board with a well-rounded focus.”

**INFORMING THE BASE**

Stith believes there are certain things for a mature board to assess as they look to grow in the future: By educating boards on the CISO role, for example, members start to gain interest in cyber, want to know whether they’re at or exceeding industry standard and better appreciate risk. Further, she’s adamant about investigating the cyber impact of any acquisitions as they’re brought in, warning that speed can backfire if the board is moving too quickly to discern the risk such growth has on cyber security.

“Boards are fairly risk-averse, but they need to determine an acceptable level of risk, so...help them assess the risk,” Stith said. “Boards must recognize that risk comes between 1 and N, not zero and N. We can’t achieve zero. But we can apply the best practice of using experts to explain to board members what matters most and why. We can help build that understanding.

“Explaining the reasoning behind a request helps garner greater compliance and understanding. People start to understand what *their* role is in helping secure the organization,” Stith continued. “If you can’t explain how it matters or why it matters in a way that makes sense, you’ll lose them. If it’s about finance, patient data, or security,
orient the conversation to the piece that matters to them, versus the metrics, and you’ll foster deeper understanding.”

CALCULATING RISK

Years ago, as cyber threats increased in frequency and impact and the board agreed it needed to place additional focus on cyber, Norton and her team decided to introduce periodic external cyber assessments, more regular external audits and risk assurance exercises.

Recognizing there is limited time for board committees to review operational decisions, Norton also created an internal Enterprise Risk Management committee to allow the board committee to focus on strategic risks and oversight. The internal management committees and board understood that while they couldn’t eliminate all risk, they could indeed detect threats sooner by making investments to counter those risks.

Erickson believes board cyber risk discussions should be aligned with business objectives and metrics should inform risks more from a business perspective: How does cyber impact the ability to achieve our objective? What are the top 10 key cyber initiatives necessary to support our mission and economic growth (e.g., velocity of maturation, defense innovation, business continuity planning, workforce education, M&A integration, third party risk management, etc.)? How do these initiatives help us become more cyber resilient? How can those impacts be described and measured? What headwinds do we face as the threat landscape evolves?

“I think that for healthcare and other organizations, too, there’s really a tendency to operate in silos. We need to break those down and work across myriad areas: IT, finance, legal, compliance,” added Norton. “We looked at enterprise risk several years ago and tried to help the board understand why we needed to go there; now, I find it interesting that this year, for their top five topics to prepare for next year, the board identified cyber security as one of those. They now understand that connectivity back to business, back to delivering patient care. They realize cyber security is not just a back-office function anymore.”

What’s important is to measure what matters: That was an early conversation with our board. There are often metrics that, when taken out of context, mean nothing. If I say I stopped a million potential attacks...well, were there 10 million? Did I miss nine million? We need to demonstrate that we’re doing what we really need to be doing. Look at every program and ask, ‘Where do we fall?’ It took work with how we measure things, but we now can easily visualize our level of risk.

—Michael Czumak, VP & CISO, Memorial Sloan Kettering Cancer Center
There are more demands than resources, so we must have transparency around decision-making. There’s this constant vigilance around when maturity is happening: Do we have an adequate road map to train our teams before we need them?

—*Tricia Julian*, Baptist Health CIO

Effectiveness ratings (how certain are you that you can protect us?) lead to confidence levels. We have found that’s more effective in communicating, because the deep dive into data is way too hard.

—*Ron Mehring*, VP Technology and Security & CISO, Texas Health Resources

In my experience, not all boards are the same, and not all EMR maturity is same. The job of CISO is different depending on where their boards are and what info they’re able to consume. Start with making sure they view cyber risk as a priority. Then: What level of detail they can look at and how much time they can spend? It varies. For us, that transition is still taking place.

—*Sanjeev Sah*, VP & CISO, Centura Health

**BUILDING ON REALITY**

Computer security professional, lecturer and writer Bruce Schneier writes, “Security is both a feeling and a reality, and they’re different. You can feel secure even though you’re not, and you can be secure even though you don’t feel it.” Similarly, at this time in healthcare, when surety cannot be overrated, risk assessments are too subjective for many boards.

CISOs have been communicating cyber security as business risk: *How does increased cloud usage raise an institution’s risk?* But until boards regularly include cyber security experts, representing risk accurately still can feel fairly unstable. Further, benchmarking one’s healthcare system against another’s might feel wise but completely miss reality: Another organization’s experience in data loss prevention doesn’t really matter. Instead, forward-thinking CISOs and boards are focusing on the risk for their specific institutions and considering their current capabilities. And should they find themselves lacking, the wisest ones will invest in those areas to shore up the whole.
C-Suite Risk Assurance/Business Continuity Management

Healthcare IT being what it is, though, means aligning fluidly to the things that matter, when they matter most—regardless of what originally was planned. Exhibit A? 2020. COVID-19 brought a flummoxing perspective to risk, in ways that few predicted; for example, as if the disease itself wasn’t confusing enough, CISOs now must reckon with vaccine supply-chain threats and EMR attacks. But even beyond the pandemic, there’s been an enormous amount of change and threat—not only impacts on continuity, resiliency and recovery, but on the ways in which mission-critical services are viewed and supported in light of ransomware, phishing and other attacks.

Ron Mehring, VP Technology and Security & CISO, Texas Health Resources, understands such shifting recovery objectives: As THR moved workers home, remote access gained a brand new emphasis, with IT studying more closely how applications were being used offsite while also communicating threats and risks differently.

“We were sending more tips on how to work from home, what employees needed to notice. Our resiliency perspective changed in this remote scenario. For example, what happens if your computer doesn’t work?” Mehring asked. “We needed a different way to get people up and running. Management had to change.”

Ron Mehring, VP Technology and Security & CISO, Texas Health Resources

Helen Mohrmann, CISO, University of Texas System

Janet Norton, Chief Legal & Regulatory Affairs Officer, Baptist Health

**ENGINEERING SOLUTIONS**

The average downtime and demand for ransomware attacks is 15 days and $112k...with some far longer and more expensive. To protect data and reputations:

**Communications/Coordination:**
1. Are you communicating threats/risks differently in your organization?
2. Are you being asked to report differently?
3. Are you measuring continuity/recovery program objectives differently?

**Continuity/Recovery:**
1. Have you evaluated clinical/business downtime procedures?
2. Have you determined leadership's appetite for extended downtime?
3. Have you evaluated and communicated recovery limitations?
4. Have you addressed integrated vendors (supply chain), partners, clinically integrated networks and joint ventures?

**Testing/Proactive Measures**
1. Have you changed the way you're performing continuity/recovery testing?
2. Have you evaluated/ integrated proactive measures to improve detection/recovery time?

<sup>1</sup>Health IT Security, May 4, 2020
As such, THR has started reporting differently on newer threats, and will evaluate its recovery and continuity objectives next year to ensure they’re still working. The focus remains on strong communications around continuity and resiliency expectations, threats around ransomware, and the like.

“Have you evaluated your clinical/business downtime procedures? We’d done all kinds of recovery events, but when ransomware started happening, we dealt with many problems,” Mehring reported. “There are various facets with ransomware, and after a few days of downtime it gets way more complicated.”

SIFTING THROUGH RUBBLE

*Complicated* is an understatement. The [New York Times](https://www.nytimes.com) reported recently on the University of Vermont Medical Center’s cyberattack in late October 2020, and the fallout was immense: It took nearly a month for UVMC to restore its EMR system. They also were forced to send away hundreds of cancer patients, and their standard operating procedures were upended, necessitating writing notes, sifting through mounds of paperwork and reconstructing complex chemo protocols from memory.

As Chief Information Security & Privacy Officer for University of Chicago Medicine, [Erik Decker](https://www.chicagomedicine.com) notes that hackers often break into both backup and ancillary systems—so medical centers face a full-down time. Further, traditional disaster recovery, originally focused on hazards and events affecting only one site, now must respond to attacks that threaten to break down an organization’s entire infrastructure.

“We have to determine which are mission-critical systems. For example, if we lose this specific information, are we out of business?” Decker asked. “We have to figure out how to build space around the backup environment for protection. This is where tape is not bad...as terrible as tape is! What you get from tape is “Write Once Read Many.” There are modern vaulting technologies that can provide the same level of protection for these mission-critical systems, which are important to consider as part of your recovery strategy to a ransomware event.”

DESIGNING CONTINGENCIES

In considering his leadership’s appetite for extended downtime, Mehring believes connecting the dots is key.

“We’ve had ransomware impact one small thing, and we’ve had impacts that would knock us down for days. We’re learning how to better communicate what it means for various tasks,” he said. “Like with paper dependencies: We’ve had issues with our e-prescribe functions working in the EHR and also found swaths of clinic doctors who’ve given up on paper scripts, so it’s good to have techniques to communicate about potential limitations.”
To force such limitations to the surface, one Health System CISO’s team planned a dramatic exercise: They gathered over 60 of their key clinical team members and staff and proposed a serious scenario: What if our technology got hit hard and went down for seven days—no phone, no fax, nothing. How would you take care of patients?

Here’s what they found, after making the clinicians bring in their downtime procedures: The newer medical team members didn’t really know how to ‘do paper’—they’d always relied on e-systems. In putting the clinical and business professionals together, they found most of the new employees didn’t know how to support and round out patient care (e.g., prescribing, charting, file sharing) without using such technology—like in the ‘olden days.’ For the CISO team, it was a good lesson learned.

Larry Yob, Interim CISO (AMITA Health) and DIS (Ascension), has seen much of the same, with the younger clinicians struggling to revert to paper while the older ones revel in it. Further, supporting and ancillary system users don’t often grasp the full impact of an outage, thinking merely that their systems are down when, in actuality, data and functionality have been wiped out.
“We’ve been looking at our core infrastructure and how resilient it is. We have three backup scenarios but still aren’t air-gapped, so it’s almost real-time replication. We’re asking: Is there a way to change, so the third copy is a little out of sync to maintain continuity?” Yob questioned. “We had some outages recently that were tough to bounce back from that had nothing to do with us but rather providers, so we’re trying to build more resiliency, focus on redundancy and plan our worst-case scenario: What do we need to run backup operations?"

Building and Managing a Risk-Awareness Culture in the Mobile Workforce

Of course, system outage repercussions aren’t limited to the physical medical center: They ripple out to impact those working from home…and those working from home also can impact (even unwittingly) system outages. To get a more accurate picture of the risks, benefits and requirements, many healthcare systems have quickly developed and/or reinforced their remote work procedures during COVID.

“We’ve been challenged during this time and, as a group, have done well and supported our organizations’ remote needs,” said Jigar Kadakia, Chief Information Security Officer & Privacy Officer, Mass General Brigham. “That said, not everyone had a laptop…so once that was managed, it’s been pretty smooth from a security standpoint. What we’re working through now is the future of a workforce that’s more remote.”

Espionage actors target COVID 19 entities (government, healthcare, pharma, medical research), with:
- increasing ransomware attacks
- focused on third-party providers
- dwelling for longer periods of time
- launching ransomware as part of a multi-pronged attack that includes data exfiltration + extortion

Common attack vetors (remote desktop access, phishing, drive-by downloads)
- Lateral movement (after initial foothold, discovery of additional vulnerabilities inside network)
- Timing, with most attacks after-hours

Teams that are part of same attack (i.e. Team A gets in; Team B maintains access)

Vision for a (Secure) Mobile Workforce:
- Shift non-essential workforce culture from statically persistent to dynamically mobile
- Leverage mobile workforce program as a differentiator to recruit/retain top talent nationally
- Consider every environment of access to be untrusted; build solutions that adopt “Zero Trust” to protect the mobile worker and data
DRAWING BETTER BLUEPRINTS

Kadakia reported that many people are working remotely and that benefits workers in a variety of ways—excellent for public-health reasons and challenging for security reasons. In MGB’s case, they’ve had to teach people different procedures (e.g., printing sensitive documents at home) that previously were no-brainers. They’ve also had to reinforce ergonomic standards in environments they’ll never see. But overall, he said, the office has been “limited,” not closed; people are quite comfortable working remotely and coming in on occasion.

Jim Hanson, ISO, Avera Health, noted before COVID hit they hosted 300 to 400 remote sessions daily, via Pulse or VMware View, with minimal “permanent work-from-home” designations. Today, they host 2,500 remote sessions daily via Global Protect, Pulse or View; are moving everything possible to Always On VPN; and are revising their telecommuting policy while wrestling with how to measure productivity in an offsite workforce.

“We, too, are seeing that printing from home, for example, is impacting our review of processes for ‘how it was always done,’” Hanson acknowledged. “Now we’ve revised our process for printing requests, approvals and overrides. We have employees sign confidentiality and HIPAA agreements and review the need annually.”

For Erik Decker, Chief Information Security & Privacy Officer, University of Chicago Medicine, their vision of a secure mobile workforce requires a solid cloud and mobility presence. The whole “anytime, anywhere” dynamic model has meant moving away from the more static You’ve got to be inside the organization; however, CISOs need to assume remote environments are dirty and work to put security strategies in place. Decker’s team believes the new IT capabilities needed to enable their remote workers entail the following.

» **Collaboration** (Office 365, IM, e-fax);
» **Communication** (cloud email, video conferencing, virtual phone and whiteboard);
» **Content** (cloud storage, electronic signatures, Office 365/SharePoint); and
» **Compute** (virtual desktop, mobile devices, remote thin clients).

Once you understand the technologies to enable the worker, then you can secure them. And for the future? Decker is focused on moving beyond the immediate needs to truly enable his mobile workforce. In his opinion, several other new capabilities will need to be introduced that are reliant on the greater IT strategy, including cloud-access security brokers (CASB), mobile-application management, data loss protection, federated access management and record retention strategies.

---

We studied how many people were connecting to the VPN on their personal devices, which was 80. But the most common risks that occur with such use were significant. We’re pushing back now on BYOD: For those 80 people? Let’s just give them a laptop and minimize risk wherever we can.

—Erik Decker, Chief Information Security & Privacy Officer, University of Chicago Medicine
CONSTRUCTING SAFETY NETS

But our experts agreed that tech security cannot be the only focus regarding mobile workers. Organizations also are recognizing the need to put as much emphasis on their workers as their work environments.

“We have all passed the technology issues and are now focused on the mental health implications. In remote work, the things that are missing—especially with those workers who are fairly new—is how to build their social networks, continue with career development and deal with the mental health issues associated with remote work,” Kadakia explained. “With the pandemic, some people have done well working remotely. Others, for whom the office provided friendships and respite, might be struggling. When you factor in multi-generational household interruptions and homeschooling requirements now, it can be difficult to work from home.”

On a national level, tactical crisis response guides tout one main suggestion: *Take care of the team*. On a local level, groups have gotten personalized and creative. Hanson’s team leverages a daily virtual huddle to connect personally as they work to maintain connectivity between individuals as they work from home. Todd Greene, VP & Enterprise CISO, Atrium Health, also does daily morning huddles that approximate normal office coffee times to ensure his workers are doing ok. “We saw some teammates struggle after six months working from home during the pandemic, and we needed to help them. We’ve got to remember we don’t know what’s happening in people’s homes; some haven’t left their houses in months. We continue to keep an eye out for them and reach out in a personal way...even as impersonal as virtual meetings can be.”

Final Thoughts

Healthcare system CISOs historically have been tasked to be organizational defenders and innovators, aiming to always stay a step ahead: As cyber-dependence grows, so do the threats (and the willingness of those doing the hacking). But also, as we’ve seen during the pandemic, these key players also have been charged with MacGyvering on the fly, establishing critical boundary lines in this Brave New Frontier of massive teleworking efforts while also tending to their teams in ways never before needed.

How to build more effective remote worksites, balancing always-on with always secured? What about designing comprehensive telework policies and procedures that offer critical cyber risk education, or keeping teleworkers engaged, invigorated and connected while mitigating BYOD risks? As CISOs continue to innovate and collaborate with the industry’s best and brightest, they’re also thankful for the sharing of knowledge and expertise, via Summits like this, that will help them plan solutions that protect their most valuable resources while serving their most valuable populations.
About the Sponsors

The Scottsdale Institute (SI) is a not-for-profit membership organization of 60 prominent, advanced, not-for-profit health systems and academic medical centers whose mission is to improve healthcare quality, efficiency and personal experience through IT-enabled transformation.

Our North Star is thought leadership guided by SI’s Three Pillars of Collaboration, Education and Networking. We convene intimate, informal and collegial forums for senior healthcare executives, including but not limited to CEOs, CMOs, CIOs, CMIOs and CNIOs, to share knowledge, best practices and lessons learned. Our goal: Gather the right people to discuss the right topics at the right moment.

For more information, visit www.scottsdaleinstitute.org.

Deloitte: Innovation starts with insight and seeing challenges in a new way. Amid unprecedented uncertainty and change across the health care industry, stakeholders are looking for new ways to transform the journey of care. Deloitte’s US Health Care Providers practice helps clients transform uncertainty into possibility and rapid change into lasting progress. Comprehensive audit, advisory, consulting, and tax capabilities deliver value at every step, from insight to strategy to action. Deloitte’s US Health Care Providers practice knows how to anticipate, collaborate, innovate, and create opportunity from even the unforeseen obstacle.

Learn more at deloitte.com