Executive Summary

The number of ways to win a game of chess are practically limitless, but they all center around strategy. Similarly, protecting a healthcare enterprise’s data operations and defeating its attackers can take myriad forms but requires the same patience, practice and cunning.

At this Scottsdale Institute (SI) virtual 2021 CISO Summit, held on December 7 and moderated by Deloitte, the name of the game was open discussion. SI gathered 18 Members from 18 organizations to talk about known, experienced and potential threats; study existing and anticipated cyber trends; and debate the merits of negotiating ransoms versus reinstating systems. Sharing wisdom along the way. Members discussed the topics of the day, including:

Effective Threat Intelligence around internal and external data sources to:
- Tune out the noise while paying attention to the signal
- Navigate staffing, skills and outsourcing decisions and share lessons learned
- Formulate incident response processes and playbooks

Enabling Security & Privacy in an Ecosystem to:
- Better assess third-party-, supply chain- and payer security
- Protect against ransomware and establish a game plan around ransoms
- Develop contingency plans with executive-level support

Ransomware Playbooks and Practice around tactics such as:
- Recovery System Security
- Detection and Response Security
- Awareness Training/Colleague Education
- Supply Chain Security
- Application & Device Security
- Email Security Optimization
- Digital Identity Security
SUMMIT PARTICIPANTS

Tina Basch, VP & CISO, Baystate Health
Jeff Bontzas, CISSP, CHISL, VP of Information Security & CISO, Ascension
George Carion, CTO & CISO, Cedars-Sinai
Michael Czumak III, VP & CISO, Memorial Sloan Kettering Cancer Center
Erik Decker, CISO, Intermountain Healthcare
Scott Dresen, SVP & CTO/CISO, Spectrum Health
Jason Elrod, CISO, MultiCare Health System
Will Hatcher, Director of Enterprise Security—Cyber Fusion Center, Trinity Health
Matt Heign (not pictured), MBA, VP & CTO & Interim CISO, UW Health
Jigar Kadakia, MBA, Chief Information Security & Privacy Officer, Mass General Brigham
Thien Lam, VP & CISO, BayCare Health System
Bryan McDowell, VP & CISO, University Hospitals
Robert Perry, CISO, Carilion Clinic
Christie Polley, CISO, Northern Light Health

Sanjeev Sah, VP & CISO, Centura Health
Pavel Slavin, VP & CISO, Froedtert & Medical College of Wisconsin
Patrick Voon, CISO, Loma Linda University Health
Vugar Zeynalov, CISO, Cleveland Clinic

CONVENER

Scottsdale Institute
Janet Guptill, FACHE; Cynthia Schroers; John Hendricks; Chuck Appleby; Karen Sjoblom; Ricki Levitan; Ishmeet Kumar; Stuart Hurley, FACHE; Margaret Shea; Courtney Olson; Genevieve Hedland-Hill; Shelby Olson; Nancy Navarrette

SPONSOR

Deloitte

Moderators:
Raj Mehta, Partner; David Mahon, Global CISO

Writer: Karen Sjoblom
Introduction

Anyone who’s ever played chess knows it’s a long exercise in strategy, as the opening game mobilizes the pieces, the middlegame advances by attacking and defending, and the endgame reveals the wiser (or luckier) opponent. Experts suggest there really are only a few key tips to help one win: Learning the moves, understanding the value of each chess piece, controlling the board and planning well. But the Shannon Number, which represents all the possible moves in a game of chess, comprises $10^{111}$ to $10^{123}$ various positions. Considering scientists estimate there are between $10^{78}$ to $10^{82}$ atoms in the observable universe, the number of ways to win a chess match and defeat one’s opponent boggles the mind.

The same is true regarding the number of ways to protect a healthcare enterprise’s data operations and defeat its attackers. The possibilities are endless...but the applications require strategy. At this Scottsdale Institute (SI) virtual 2021 CISO Summit, held on December 7 and moderated by Deloitte, the name of the game was open discussion. Eighteen Members from 18 healthcare organizations considered known, experienced and potential threats; studied existing and anticipated cyber trends; debated the merits of negotiating ransoms versus reinstating systems and far more, with the end result depicting any number of IT security “moves” that may or may not produce a victory. But as in most things, such a victory would be short-lived, as these CISO professionals are, by nature of the job, always looking ahead and strategizing their next steps.

Moderator Raj Mehta, Partner, Deloitte, kicked off the Summit by reviewing some of today’s broad cybersecurity trends in healthcare, including:

- **Unlocking the potential of data:** Securing interoperable and open platforms for innovative services and delivery models, maintaining security and privacy while sharing and aggregating data
- **Securing cloud-enabled transformation:** Developing scalable, flexible and resilient cloud cyber solutions, and recruiting and training talent with the right skills
- **Establishing digital identity management:** Putting patients and communities at the center to provide a seamless experience and in-time access along with driving increased maturity and scaling for managing workforce member access while balancing experience and security
- **Connecting to the Internet of Medical Things:** Realizing that greater connected device adoption will drive care delivery but also require device trust and security management
- **Monitoring the continued threat of ransomware:** Assessing and integrating attack risk into enterprise risk and crisis management procedures while creating a playbook to detail incident response
- **Continuing on the Zero Trust path:** Managing risk while supporting the need for workforce mobility and flexibility
- **Overcoming talent challenges (automation, outsourcing):** Finding talent with the right skills to secure contemporary business requirements and managing risk associated with the larger/global vendor landscape
- **Conducting meaningful cyber executive-level reporting:** Identifying metrics, measuring and communicating the effectiveness of security investments and aligning messages with the integrated enterprise risk management approach
- **Managing vulnerabilities across the technology stack:** Prioritizing assets, keeping pace with tools and integrations and paying attention to legacy and end-of-life software challenges

There’s a perfect storm looking at cyber talent demand versus supply and cost (going up). This combination is not sustainable. Within the cyber function, some systems are looking to build a focus area whose sole focus is looking at opportunities across cyber to boost efficiencies.

-Raj Mehta, Partner, Deloitte
Effective Threat Intelligence

With a network of 11 hospitals, MultiCare is a not-for-profit healthcare organization that’s been caring for communities in Washington state since the founding of Tacoma’s first hospital in 1882. Boasting over 20,000 employees, providers and volunteers, MultiCare has grown from a Tacoma-centric, hospital-based organization into the largest, not-for-profit, community-based, locally-owned health system in the state of Washington offering inpatient, primary, virtual, urgent, dedicated pediatric and specialty care. Navigating threats is a key part of Jason Elrod’s job as MultiCare’s CISO, and thus how he chose to kick off the Summit’s first open discussion—with both a clarification and a question.

In considering cyber-threat intelligence (CTI), Elrod believes sources include intel from myriad directions: industry experts, open source, social media, humans and tech, device log files, forensically acquired data, dark web findings...basically anywhere people or information flows. But with such a wide breadth of information, how are professionals using it to protect their data? “If we have all the things listed in this poll question (below), how do we use them effectively? What systems and models are being implemented to manage the depth, breadth and volume of threat intel we receive in our organizations?”

Elrod questioned the group on how to use people, processes and technology as a force multiplier to make CTI more frictionless, as well as how to separate the signal from the noise—that is, determining what’s important to the organization, versus the industry, versus the larger global community.

<table>
<thead>
<tr>
<th>CISO Summit Poll Question 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. What are the biggest challenges related to effective Threat Intelligence? (Single Choice)</td>
</tr>
<tr>
<td>Getting relevant and timely intelligence</td>
</tr>
<tr>
<td>Operationalizing intelligence</td>
</tr>
<tr>
<td>Ability to find and hire skilled staffing</td>
</tr>
<tr>
<td>Executive support for budgeting</td>
</tr>
<tr>
<td>Effective Technology Solution(s)</td>
</tr>
<tr>
<td>None of the Above</td>
</tr>
<tr>
<td>All of the Above</td>
</tr>
</tbody>
</table>
“What’s happening in the industry versus to us locally? How can we determine what to implement here?” Elrod questioned. “We must consider the entirety of that threat intel against what’s important to us specifically.”

**With CTI, we have to consider our vendor partners as well as cyber liability insurance companies. Who offers those tighter relationships that you can benefit from and leverage? For us, it’s our insurance partners. They make sure we’re getting the right info at the right time, not three months later when they think a compromise might have occurred.**

-Tina Basch, VP & CISO, Baystate Health

I have 117 people on my team now, with 132 expected in 2022, all dedicated to threat hunting. But the question is, unless you have the people and processes (people first), how realistic is it to do this at any kind of scale, with any kind of real value that you can bring back to the organization?

-Erik Decker, CISO, Intermountain Healthcare

For us, building a relationship with local law enforcement was very beneficial, because NYPD and the local FBI have pretty robust threat intel available. We’ve also leveraged third-party info, feeding analysts’ data and correlating it with other data to pinpoint the threats that are most timely and relevant for us. We also track threats through mediation and mitigation activities, which has been helpful from a historical perspective. As new threats come out, we ask, “Have we seen this before?” We’ve brought on a dedicated resource who’s getting a masters in threat intel now and is helping to lead and build out that functionality.

-Michael Czumak III, VP & CISO, Memorial Sloan Kettering Cancer Center

**WINNING MOVES: EXTERNAL VS. INTERNAL THREAT INTELLIGENCE SOURCES**

Elrod queried the group on where the most value is being generated and whether they’re taking advantage of crowdsourcing awareness of anomalous activity or info-sharing with other organizations. “There are sources within the organization where you can take advantage of tribal knowledge, such as when the Service Desk notices anomalous trends and requests,” Elrod explained. “We all have resources like this internally and externally, so what are your thoughts about hacking them and crowdsourcing the intel toward cybersecurity efforts?”

_The hard part is getting actionable intel from this data. It’s taken us a couple years to get to the “actionable” part. Also, it helped to get focused with a threat-hunting program—daily or weekly, giving them the landscape of what to look for. We started with the tools, and the tools provided the data (which felt a little like searching for a needle in a haystack), but what really helped was meeting with this group and coming up with processes._

-Will Hatcher, Director of Enterprise Security—Cyber Fusion Center, Trinity Health

We have simulated threat intel, but if you don’t already have a partnership with someone who has a relationship in the deep web, I’d recommend it. We have someone scanning for us—for emails and other details—and if you’ve had a persistent attacker trying to infiltrate your organization or saying they’ve stolen credentials, you can have your partner negotiate for you. It’s very helpful if you have limited resources and have to focus on prioritized action.

-Jeff Bontsas, CISSP, CHISL, VP of Information Security & CISO, Ascension
Elrod then asked, “We’ve implemented a threat intel cycle (right) for continuous improvement, and are using that to shift left in our program and mitigate vulnerabilities quicker and more efficiently. How do you handle exploitability of vulnerabilities in your environments, and how are you using threat intel? Proactively, reactively. Incident Response, academic?”

We have a dedicated team of three on threat intel, monitoring the deep web; if they find certain credentials, that trips our password reset program, for example. We also have board presentations around global, industry-specific and local threats and how to manage them, as well as fusion center/team exercises to stay current.

–Vugar Zeynalov, CISO, Cleveland Clinic

In northeast Ohio, all the big companies based here, like Progressive Insurance, Rocket Mortgage, Charles Schwab, etc., pull together through a tip program and share intel there.

–Bryan McDowell, VP & CISO, University Hospitals

Because we have only four people on our team to assess threats, we’ve also had a cyber insurer on retainer and a forensic firm that’s jumped in quickly when needed. But it became very apparent that endpoint detection response was one piece we really needed; we were looking to implement it but due to financial constraints didn’t...and while we thought we had enough protection without it, we were wrong. We now rely on a Managed Security Service for endpoint detection and response, and are trying to enable and improve central logging to get a more complete, comprehensive picture. It’s been a journey, but in terms of supplementing our capabilities, that was the way for us to go.

–Patrick Voon, CISO, Loma Linda University Health

In the end, Elrod notes that by the time health systems find they have a nefarious “insider,” it often can be too late. The longer their presence, the longer time they’ve had to learn the ins and outs of the environment. But by strategizing ahead of time according to their health system’s specific challenges, intel and partnerships, these professionals can envision and implement their next moves to stay a step ahead.
Enabling Security & Privacy In an Ecosystem

Founded in 1994, Partners HealthCare (now Mass General Brigham) coalesced Brigham and Women’s Hospital and Massachusetts General Hospital, two of the nation’s leading academic medical centers with histories dating back to 1832 and 1811, respectively. Today, 16 member institutions comprise a range of healthcare organizations (academic medical centers, specialty hospitals, community hospitals, a rehabilitation network, a health insurance plan, a physician network, a teaching organization and myriad locations for urgent and community care). With such a far reach, Mass General Brigham is especially cautious around its third-party-, supply chain- and payer security. On this front, Chief Information Security and Privacy Officer Jigar Kadakia began this discussion by recapping the poll question (right).

“While we’ve focused on cloud risk, we feel those are manageable. But when we focus on third-party- and supply chain risks, I think there’s much to consider and that we could benefit from collaborating together,” Kadakia said. “As an example, just in the last week there have been three major ransomware occurrences. Between physician billing, reimbursements, call centers and the like, these third-parties’ vulnerabilities impact our activities. We then have to cease services while they deal with ransomware problems, and it’s happened frequently over the last six months. What can we do, as a group, to learn about and protect ourselves from this core third-party risk?”

According to HealthcareIT News, 2021 “…has been a particularly dire year for healthcare data breaches, with incidents taking down networks for weeks at a time and potentially leading to disruptions of care throughout the country... Overall 40,099,751 individuals’ records have been affected by exposures reported to the federal government so far this year.” HIPAA’s May 2021 Healthcare Data Breach Report noted 63 breaches of 500 or more records in that month alone, with the average number of breaches per month rising to nearly 55. Furthermore, in a September 10, 2021, piece, Security Magazine blogger Vinay Gokhale wrote, “Chief security officers and other stakeholders protecting the integrity of healthcare organization supply chains face growing challenges. Smarter, connected

READ ALL ABOUT IT
supply chains carrying a flow of smarter, connected devices may simplify management and improve efficiency, but they also bring security risks in this Internet of Medical Things (IoMT).” Then, Fierce Healthcare suggested that even providers with robust cybersecurity programs are struggling to secure their supply chain systems, all while BusinessWire reported on CynergisTek’s claims that 76 percent of healthcare systems failed in securing their supply chains, and these are just a few reports from recent months.

Kadakia reminded his peers that such attacks can come from myriad directions, with multiple levels of impact, including:

- **Supply chain risks** (e.g., personal protective equipment, medical supplies) that, while not security-related, still pose a challenge;
- **Third parties receiving health system data** that can be impacted by a ransomware event; and
- **Ancillary businesses** not normally associated with “healthcare” per se.

For the latter, Kadakia shared thoughts about recent security breaches and ransomware attacks that crossed geographical boundaries and directly impacted Mass Brigham, causing them to stop work for a time while those third-party vendors managed the fallout.

- **Hoya Optical** (third-party-managed lens and glass shop located within Mass General Brigham)
- **Mass Eye and Ear** (multiple breaches and fines)
- **Shawmont Printing** (EOB statements)
- **LogicGate** (risk and compliance via Amazon Web Services)
- **Elekta** (oncology database)

Recognizing this is a never-ending battle for health systems, Kadakia opened a discussion around mitigating threats, navigating intel and learning what’s worked to keep tech systems and data safer.

*We faced Elekta as well, and just learned from dark web scanning that an ancillary arm of the business had ransomware activity in November, so we’d had a completely unknown threat space and a vendor being quiet about it. As we move mission-critical care data over, a threat like this could take us down. When we get these stacks 100 percent in the cloud, it’s hard to bring on-prem contingencies back over. This is something we have to get into, especially around critical care issues.*

–Erik Decker, CISO, Intermountain Healthcare

We try to be involved on the front end to ensure proper contracts and the like, but the real question surrounds ongoing monitoring of the vendor. Even with super great security reviews, the truth is most of these vendors would have passed any weaknesses we would have expected. But with ransomware activities...what do you do after the fact? We have to come up with an alternative business solution after this happens to them. It’s like, you know it will happen, but they don’t have an alternative solution. And you can’t turn their solution back on because of the threat to the enterprise.

–Jigar Kadakia, Chief Information Security and Privacy Officer, Mass General Brigham
This is what keeps me up at night—this interdependence with third parties. We tend to look at our engagement just in the beginning—it’s like, “Should I date this partner?” Then we get married and we don’t talk but once a year. But it’s all the stuff that happens in between: How do we know this is still a good relationship and doesn’t present outsized risk to critical care? Some vendors want to redline their notifications to us when they have a breach, saying “I don’t owe you anything.”

–Jason Elrod, CISO, MultiCare Health System

We handle such things within InfoSec since we have to do risk assessments. We do analysis and based on the result we make decisions that may impact the business. We make a determination based on the third party; some are very clear, some are very gray. In most cases, we’re handling many different parts of the response.

–Jigar Kadakia, Chief Information Security and Privacy Officer, Mass General Brigham

When we conduct risk assessment of third parties, our key discussion now is really talking through what happened and when. It’s not a business continuity issue; in fact, I’ve been notified of two vendors having issues while I’ve been in this Summit! You need to consider what you’re going to do if your service goes down: Will you pull up downtime procedures? Do you have other vendors in mind? Nine times out of 10, the answer is no.

–Tina Basch, VP & CISO, Baystate Health

We’ve uncovered fundamental problems with vendors that have driven our decision to not be in business with certain folks. Short of me managing their security operations, there’s no way we can prevent problems from happening. We have to be focused on business continuity and alternatives. There are many things that can cause a business to stop functioning—that’s why I’m pushing this as a much larger operational resilience/business continuity problem.

–Michael Czumak III, VP & CISO, Memorial Sloan Kettering Cancer Center

Third-party risk assessment questionnaires and screening tools must do a good job at shedding light on vendor risk areas and potential impacts. It’s all kind of falling on InfoSec leadership to be responsible around engaging with vendors and having those hard conversations.

–George Carion, CTO & CISO, Cedars-Sinai

We work with compliance and other folks to determine whether there’s a clean bill of health after a third party experiences a breach. But after severing that connection for your own safety, what are your criteria to restart that relationship? Knowing that ahead of time helps.

–Vugar Zeynalov, CISO, Cleveland Clinic

We deal a lot with Legal and Supply Chain; they have a list of vendors we can use and we hold the line on them… but it’s not foolproof.

–Bryan McDowell, VP & CISO, University Hospitals
Ransomware Playbooks & Practice

“Our board requires we protect ourselves against ransomware via seven tactics,” reported Will Hatcher, Director of Enterprise Security and Cyber Fusion Center, Trinity Health.

Based in Livonia, Michigan, Trinity Health is one of the largest not-for-profit, Catholic healthcare systems in the nation, with 115,000 colleagues and nearly 26,000 physicians and clinicians caring for diverse communities across 25 states via 88 hospitals, 131 continuing care locations, 125 urgent care locations and many other health and well-being services. With such an extensive impact, Trinity’s security teams have their hands full ensuring their systems keep running without interruption. Toward this end, Hatcher delineated Trinity’s seven tactics more fully so Summit participants could clarify their own key objectives and mitigations as well.

1. RECOVERY SYSTEM SECURITY

Objective: Stop the deletion or corruption of file backup systems and detect mass data exfiltration from file systems.

Mitigations:
1. Perform automated system and file change backups
2. Monitor and protect file backup systems
3. Protect the SAN administrator password
4. Employ SAN user monitoring system that alerts anomalous file activity

Highlights:
- Monitored backup
- Separate backup and system password
- Immutable backup
- Restore checked prior to putting back on system
- Multiple multifactor authentication (MFA) challenges for administrator

Regarding immutable backups: We archive data either through replication or software-controlled backup processes to a cloud provider. We control our cloud data protection policies so that archives cannot be overwritten at any point during a retention period, even by a person with the cloud provider admin keys. This isn’t inexpensive, but it’s a way to ensure that nobody can touch the data.

–George Carion, CTO & CISO, Cedars-Sinai

2. DETECTION AND RESPONSE SECURITY

Objective: Detect ransomware malware early and block its execution.

Mitigations: An EDR that detects and/or blocks...
1. Instances of system penetration software (Cobalt Strike, Powershell Empire, Bloodhound, Mimikatz and Lazagne)
2. Dangerous and unusual Powershell scripts
3. Suspicious processes and registry operations

Highlights:
- Prevents execution of malware and allows team members to pivot and gain network access
- Revealed aforementioned strange behavior after running a Powershell script
- Avoided ransomware for the past four- to five years via Crowdstrike
3. AWARENESS TRAINING/ COLLEAGUE EDUCATION

Objective: Train users to detect and report suspicious emails and other activities.

Mitigations: A constantly scheduled security awareness campaign that:
1. Holds phishing exercises regularly to educate clickers on how to detect and report phishing emails
2. Requires annual security awareness training to update colleagues on threat tactics and how to report suspicious cyber activity
3. Conducts ransomware cyber-exercises (especially for executive critical decision matrix around shutting down services and paying ransoms)

Highlights:
- Notify manager if someone repeatedly falls for phishing emails
- Employ Helpdesk as “the canary in the coalmine” to prevent against easy access

4. SUPPLY CHAIN SECURITY

Objective: Ensure VPNs, remote access accounts and shared network devices are secured and protected to prevent ransomware attacks via vendor accounts or networks.

Mitigations:
1. Secure remote access solution for partners and vendors that limits access to only needed devices, monitors activity, utilizes MFA and doesn’t give admin access to the network
2. Conduct risk assessments on vendors and partners
3. Issue security requirements for future vendor and partner contracts and agreements (EDR)

Highlights:
- Understood that remote access to an environment requires understanding connections; having a current inventory of VPN connections to the environment is a requirement
- Limited access to only necessary devices for greater protection
- Recognized that an even bigger threat than recovery was release of patient data on the dark web

We’ve built into our playbook the established roles, decision-makers, backup decision-makers, third-party reports, external cyber-council, etc. We’ve engaged with insurance carriers and thought through and exercised every step. All those things should have been decided already, with everyone—key decision-makers, board members, everyone—knowing their roles ahead of time. If you have other vendors or intel sources, they might be part of your response process as well.

–Michael Czumak III, VP & CISO, Memorial Sloan Kettering Cancer Center

We have a similar approach; we developed high-level guidance to help make those decisions to pay or not to pay. The most obvious case to paying is, can you get to patient care faster? Or can we deal with the disorganization and get back online faster if we worked it out ourselves? We also consider that ransomware can affect a single floor in a building or multi-hospital system and, based on those factors, we determine whether paying a ransom would be appropriate.

–Pavel Slavin, VP & CISO, Froedtert & Medical College of Wisconsin

We’re presenting different scenarios to the board in February since it’s a board-level decision to pay ransoms or not. But we’re also bringing in an insurance broker as well to show what’s happened to others. That intel around ransomware families and how trusted they are—whether recovery keys would be valid, whether we could use de-encryption capabilities—is crucial. Who can you trust to say, “Yes, you can trust this family and this is the encryption key” or “No, we have to go through the backups even though it will take time”?

–Tina Basch, VP & CISO, Baystate Health
5. APPLICATION & DEVICE SECURITY

Objective: Secure network devices from known vulnerabilities to make exploitation harder.

Mitigations:
1. Employ network vulnerability scanner that reports systems with known vulnerabilities, OS versions and patch levels
2. Conduct network segmentation for those devices that cannot be secured (e.g., medical and/or vendor devices)
3. Have reboot and patch SLAs for servers and critical systems

Highlight:
- As part of the vulnerability process, ensure reboots are tracked and reported because some patches do not provide coverage until a system reboot occurs

6. EMAIL SECURITY OPTIMIZATION

Objective: Allow fewer suspicious emails to reach inboxes (inbound email) and better protect users from clicking on malicious links.

Mitigations:
1. Employ a commercially recognized mail gateway to filter spam and known hostile links
2. Use Microsoft M365 Defender (formerly ATP) to examine attachments, links and sender reputation
3. Increase junk mail and phishing protection levels in Outlook
4. Enable safe links for Exchange, which evaluate for malicious content using M365 cloud-based analytics
5. Employ branding update to External Notification Banner and commit to review annually
6. Share optional guidance on how to create an email rule that redirects external emails to separate folder

Highlight:
- With the use of consumer platforms that provide these capabilities (e.g., Gmail or Hotmail), the impact to the user experience is low

7. DIGITAL IDENTITY SECURITY

Objective: Protect and verify user identities when logging into the network or application.

Mitigations:
1. Enforce MFA for all remote access
2. Enforce and change complex passwords
3. Protect admin passwords through password vault and MFA
4. Limit ability to change MFA devices to on-network or help desk
5. Utilize User Behavior Analytics account monitoring to detect unusual user login activities

We’ve had lots of people traveling out of the country due to COVID (e.g., taking care of family members) and many are getting blocked when they try to log in. We’ve been saying that personal VPNs are out of the equation, but we’ve got to let our team members be with their people in times of need.

-Tina Basch, VP & CISO, Baystate Health

One of our best decisions was to move to Proofpoint. You get a report of phishing and have a password reset within 15 minutes. It’s happened even while I’ve been on this call.

-Bryan McDowell, VP & CISO, University Hospitals
Conclusion:

Wrapping up the time together, co-moderator David Mahon wisely noted, “I try to tell my team that we shouldn’t have lessons learned that someone else has learned already. We need to have a CISO network and be able to call on them: Call the ones who have robust programs and tell them, ‘Give me the deep dive on what you did or didn’t do, what worked or didn’t.’” Similarly, in the end Summit participants agreed that having the ability to discuss their common ideas, issues and struggles helps to provide insight into strategy and direction to movement. And in looking to succeed in the long game of cybersecurity, every single step is critical.