Scottsdale Institute 2017 Chief Information Security Officers Fall Summit

Best Practice Standards in Cybersecurity Risk Management

October 18–19, 2017 | Chicago, IL

Sponsored by:

SCOTTSDALE INSTITUTE
COLLABORATION • EDUCATION • NETWORKING

Deloitte.

Executive Summary

Thirteen Chief Information Officers (CIOs) and Chief Information Security Officers (CISOs) of leading health systems convened in Chicago to discuss key challenges, best practice standards and collaborative opportunities in cybersecurity. These healthcare executives focused on cybersecurity maturity levels, governance practices, reporting systems, threat monitoring/threat analytics tactics and the importance of tying cybersecurity metrics to business impacts. This report captures their discussion and shared insights.

CHIEF INFORMATION SECURITY OFFICERS FALL SUMMIT PARTICIPANTS

- **Fernando Blanco**, Vice President and CISO, CHRISTUS Health
- **Jeff Bontsas**, MS, CISSP, Vice President and CISO, Ascension Information Services
- **Erik Decker**, Chief Security and Privacy Officer, University of Chicago Medicine
- **Jim Hanson**, Information Security Officer, Avera Health
- **Bryan Kissinger**, PhD, Vice President and CISO, Banner Health
- **Thien Lam**, Vice President and CISO, BayCare Health System
- **Ken Lawonn**, Senior Vice President and CIO, Sharp HealthCare
- **Leonard Levy**, MBA, CISSP, CISA, Vice President and CISO, Spectrum Health
- **Christie Polley**, CISM, System Director, IS Information Security, Eastern Maine Healthcare Systems
- **Brad Sanford**, CISO, Emory University
- **Randy Thompson, MD**, CMIO and Interim CIO, Billings Clinic
- **Jim Veline**, Senior Vice President and CIO, Avera Health
- **Brenda Williams**, Vice President Technology Services, Mosaic Life Care

ORGANIZER: SCOTTSDALE INSTITUTE

- Chuck Appleby
- Jean Appleby
- Janet Guptill
- Gordon Rohweder
- Cynthia Schroers
- Shelli Williamson

SPONSOR: DELOITTE

- Anand Dedhia
- Tom Foley
- Unna Narayanan

MODERATORS: DELOITTE

- Bruce Daly, CISA, CISSP, CBCP, CRMA, CIA, Principal, Deloitte & Touche LLP
- Raj Mehta, CPA, CISA, CISSP, CIPP, HCISPP, Partner, Deloitte & Touche LLP

WRITER:

- Shelley Ducker, Shelley Ducker Communications

Introduction

With numerous high-profile security events and data breaches splashed on the papers of national newspapers, there is a growing appreciation in healthcare and non-healthcare organizations alike that cybersecurity impacts business as a whole. Today, cybersecurity is increasingly regarded not as a technical issue pigeonholed in IT departments, but as a corporate and business issue. The cybersecurity function is rapidly evolving, eliciting greater visibility across healthcare systems and drawing increased attention from boards and leadership charged with risk management.

In October, leadership representing Information Technology (IT) and Information Security (IS) functions from Scottsdale Institute member health systems came together to share their perspectives, experiences and strategies for tying cybersecurity metrics into business impacts and business risk and for monitoring and managing ever-changing risks and threats.

The Imperative of Linking Cybersecurity Risks to Business Impacts

There is a growing appreciation across boardroom tables that cybersecurity is a business risk, not just a technical risk. Yet, the process of reporting metrics has not fully caught up. To drive the understanding home that cybersecurity addresses key corporate and business issues, alignment of cybersecurity reporting to business impacts is key. "How many of you are regularly using business risk to report?" asked discussion moderator Raj Mehta of Deloitte, kicking off a spirited conversation focused on improved communication of metrics, risks and impacts to management and boards. "If there is a cybersecurity risk to the organization, it is fundamentally a business risk. On this, we all agree. But is it being reported up and out that way?" Mehta challenged.

Participants around the Summit table voiced challenges, shared tips and broadly agreed that CISOs and cybersecurity teams have work to do internally to better align cybersecurity metrics, measures—and even budget requests—with business risks and business impacts. Many have already started that process.

WHAT WE CONSIDER CATASTROPHIC MAY BE VERY DIFFERENT FROM WHAT THE BUSINESS CARES ABOUT

It is crucial to understand what critical or catastrophic impact means to your business leaders, emphasized Erik Decker, Chief Security and Privacy Officer at University of Chicago Medicine. "What we in IT think of as catastrophic can be very different from what the business cares

AT THE FOREFRONT
UChicago Medicine

"What we in IT think of as catastrophic can be very different from what the business cares about."

– **Erik Decker**, Chief Security and Privacy Officer, University of Chicago Medicine

about," said Decker, citing his experience in collecting feedback from his senior leadership on the business impacts most important to them.

"Early on in my program, we convened our C-suite to make objective statements around the stratification of risks that were most concerning to them and that had the most consequential impacts to the business. We talked through many different scenarios of cybersecurity risk and threat outcomes that could happen, and together we categorized and stratified these on a 1-5 scale of catastrophic to nominal. Items on the table ranged from a simple phish, to hacking that could lead to data loss, as well as cyber actions that could cause death. There is now a clear sense internally of what the most concerning business impacts are, and we can now measure and stratify risks/threats against those stratified impacts."

Core business impacts ranked by University of Chicago, and agreed upon by participants around the table, included:

1. Patient safety issues/harm to patient
2. Ransomware that can bring down digital operations and systems
3. Breach of private data
4. Mishandling of sensitive information
5. Risks/unknowns brought by M&A activity

There were hearty nods of agreement centered on the categories of business impacts, with the understanding that different boards may rank the importance of each type of impact differently.

"We have one risk measure that is a roll-up of several related risks that could impact the confidentiality or integrity of our data, and another one that focuses on the availability of our systems including business continuity and our ability to recover in the event of a disaster."

– **Brad Sanford**, CISO, Emory University

Brad Sanford, CISO at Emory University, reported that his organization reflects these business impacts in a slightly different approach. "We have one risk measure that is a roll-up of several related risks that could impact the confidentiality or integrity of our data, and another one that focuses on the availability of our systems including business continuity and our ability to recover in the event of a disaster."

CYBERSECURITY: A ROW IN A WORLD OF COLUMNS

Bryan Kissinger, CISO of Banner Health, noted that his organization views cybersecurity metrics via the lens of "confidentiality, availability and integrity of systems." Yet, he noted, none of the frameworks adequately fits the depth and breadth of cybersecurity risks and impacts. "Cybersecurity is a row in a world full of columns," he opined, in a statement that became a mantra during the Summit. "Patient safety is a column. Financial performance is a column. But security is a row that cuts across everything. Information security and cybersecurity cut

across every one of those business impacts. We are a row in a world full of columns. The row is being driven by info security and privacy teams but it permeates all of the organization and its entities."

Risk Assessment: Shaping Risk Postures through the Lens of Threat Actors

Though risk assessment is tackled differently across organizations, the value of understanding "threat actors"—and the type of impact each could have on business—was discussed as a meaningful way to approach risk assessment frameworks. One participant identified a white paper "**Hacking Healthcare IT in 2016: Lessons Learned from the OPM Breach**" as a particularly helpful resource to overlay the intentions of threat actors with the business risks of health systems.

The paper, which categorizes risks across five main categories of threat actors—script kiddies, hacktivists, cyber criminals, cyber terrorists and nation-state actors —has "helped shape our risk postures," the participant explained. "We've built a framework that considers who the actors are, what their motivations might be, and how our strategies can address those specifically. We now tie threats back to risks, and tie risks back to groups of threat actors. Today, as we profile risks and add controls, we keep the common threat actors in mind."

TIP: To manage the sheer volume and immensity of risk assessment and risk analysis, Leonard ("Lenny") Levy, Vice President and CISO, Spectrum Health, reports that he and his team balance breadth and depth when conducting their annual risk assessment. "Since it would not be feasible to go in-depth across our entire environment, we perform an enterprise assessment looking at key risks and control and once a month perform a deep dive into a specific application, location and business unit, to make a more comprehensive analysis."

SPECTRUM HEALTH

"Since it would not be feasible to go in-depth across our entire environment, we perform an enterprise assessment looking at key risks and control and once a month perform a deep dive into a specific application, location and business unit to make a more comprehensive analysis."

– **Leonard Levy**, MBA, CISSP, CISA, Vice President and CISO, Spectrum Health

Threat Monitoring

There is abundance—and many times, an overabundance—of data feeding into the threat intelligence and threat-monitoring funnel. A challenge that many agreed on is deploying the right level of internal and external resources to collect the optimal information. Outsourcing and collaboration rose to the top as the trends that CISOs are converging around.

CISO INSIDER INSIGHTS / TIPS FROM THE TRENCHES:

- **Outsourcing:** "We recently converted to a hybrid model. Our primary level 1/level 2 monitoring is now outsourced. We still retain some resources internally who respond to issues and double-check our provider. This is where our red team comes in to test and make sure it is functioning properly." (Lenny Levy, Spectrum Health)
- **Collaborative learning through ISACs**: "The information-sharing and analysis centers (ISACs) are helpful as members are able to share information about what we are seeing. After all, it only takes one person to figure out an interesting nuance to a particular threat. Then, this can be shared and everyone can take advantage. Working with ISACs, you don't need to figure out everything on your own." (Brad Sanford, Emory University)
- **Monitoring for threats not experienced…yet**: While this is an area that is ripe for maturity, many CISOs have their teams on a variety of chat rooms to "monitor what is happening externally, so we know threats we haven't experienced. You need to look for it, as it doesn't come to you." (Jim Hanson, Avera Health)
- **Structured internal teams**: "We have a team that is structured to focus on three core areas: threat management, vulnerability management, and incident management." (Brad Sanford, Emory University)
- **Establishing internal norms and flags**: "We feed privacy and access data in SIEM [security incident and event management] and determine what is normal—for example, how many records people access per day, per week and per month. So if this number of records went up, that is a flag for investigation." (Thien Lam, BayCare Health System)

Common challenges underlying threat monitoring identified by participants include:

- Cost of threat intelligence investments vs. value
- Scope
- Use cases
- Talent
- Maturity
- Intelligence

While SIEM systems were broadly regarded as the go-to tool for threat monitoring and analysis, understanding and applying the data generated by SIEM remains an area CISOs struggle to best interpret.

"As you deploy tools, you will see more [incidents]. So, it may seem like you are doing worse, but really you are doing a better job. There are not necessarily more threats, but you are expanding the visibility across your network and identifying more threats," commented Jeff Bontsas, Vice President and CISO, Ascension Information Services. Many are moving to playbooks and use cases to bolster and build out general threat intelligence.

Needed: A Plan for Ransomware across the Entire Health Sector

CISOs probed each other for what their plans were in a ransomware situation. While the commonly accepted best practice is not to pay, CISOs around the table understood that the amount of money was trivial compared to an EMR system being taken down. One CISO had even researched an investment in bitcoin to have readily available if needed—"although the board shot down that option."

This is an industry and sector issue, rather than an individual organizational issue and threat, argued Jim Veline, Senior Vice President and CIO of Avera Health. "Once one [organization] pays, we are all more likely to get attacked. It would be worthwhile to run this up the flagpole with our professional associations and generate a position paper that you do **not** pay. That gives cover and backstop to a CEO and board when faced with a difficult decision. Right now there may be FBI advice, but formal positions are lacking in the relevant professional groups we all participate in." This suggestion was met with broad agreement from participants around the Summit table, who agreed to have follow-up discussions regarding how to best raise the issue through targeted professional organizations.

Avera

"Once one [organization] pays, we are all more likely to get attacked. It would be worthwhile to run this up the flagpole with our professional associations and generate a position paper that you do **not** pay."

– **Jim Veline**, Senior Vice President and CIO, Avera Health

Reporting Business Risk: The "So What?" of Metrics

There was little consistency in the types of metrics—the key performance indicators (KPIs) and key risk indicators (KRIs)—reported up to management councils, board committees and executive boards. Summit discussions also pointed to little consistency on the frequency of reporting (some monthly, some quarterly, others annually—depending on the organization, and the body being reported to). However, there was broad agreement on the challenges of collecting actionable, instructive KPI/KRI data.

Shared challenges to developing good-quality, standardized KPIs/KRIs included the need to address these areas of variability:

- Data availability
- Data consistency
- Data quality
- Reporting thresholds

When it comes to KPIs and KRIs, there is a lack of standards guiding the industry in this field. "Management made investments in security, and we need to show the value of that investment.

But how do you best do that with today's KPI and KRI metrics?" challenged Ascension's Bontsas. "For example, we can show the increased number of attacks we blocked. Yet, it's hard to talk about value when we talk about risk avoidance. Was it worth it? What did we avoid? Telling the story of what we avoided can be difficult."

While the core concern voiced around the table was the overall lack of KPI/KRI standards guiding the cybersecurity field, the key issue that emerged was the **actionable nature** of metrics: the "so what?" factor.

COMMON CYBERSECURITY METRICS BEING TRACKED

- Encryption
- Vulnerability Management
- Patching
- 2-factor authentication
- Phishing
- Training
- Risk assessment
- CAPs (Corrective Action Plan)
- Old/Outdated legacy systems (cannot be patched)
- Identity & Access Management/ Privilege Access Management
- Incidents
- SLA (Service Level Agreements)
- SOC (Security Operations Center)

There are many KPIs "that are important for operations people, but that are not meaningful in terms of making informed decisions about risk. There are also many that are more focused on justifying spend than on risk. The challenge we face is, what is most meaningful?" noted Fernando Blanco, CISO of CHRISTUS Health. "We regularly report on metrics like 'we did patching X months ago and we hit X percent.' If we are at 85% or even 95%, is that good or bad? That is what we have to ask as we are collecting metrics both for ourselves and for the purposes of reporting up and out. However, today we lack clear thresholds to make the numbers meaningful." Summed-up by Banner Health's Kissinger: "Every metric has to answer the question 'so what' to be meaningful from a business-impact perspective."

"When there is a significant new threat that emerges, at the end of the day the 'so what' metrics we need to know are: (a) how quickly can we frame the specific risk to our institution, (b) how exposed we are, and (c) how quickly we can react and get controls in place. These are the metrics that matter most from a business perspective, and we are working now to really shrink the time for that process," said Emory University's Sanford.

KEY TAKEAWAY: A key action-item from the discussion was to ensure that, no matter what metric was being tracked, it tied back to business risk so that its value could be better understood in the broader context of business impacts. "My metrics today are not all explicitly tied to business risk, but that is what I am going to go back and do," reported Randy Thompson, MD, CMIO and Interim CIO, Billings Clinic, to the team.

Billings Clinic

"My metrics today are not all explicitly tied to business risk, but that is what I am going to go back and do."

– **Randy Thompson, MD**, CMIO and Interim CIO, Billings Clinic

THREATS, RISKS AND METRICS: CISO INSIDER INSIGHTS/ TIPS FROM THE TRENCHES

- **Collaborate with outside parties/external auditors:** "We do both internal and external risk assessments. We have internal auditors that check for risk/cyber risk. Then we hire and have high-tech security firms audit so we have a different set of eyes every year." (Brenda Williams, Mosaic Life Care)
- **Outsourcing and hybrid models:** "Our small team couldn't move at the pace the business needed, so it made sense to outsource rather than hire in. The funnel was too small internally to send all the third-party risk assessments through." (Lenny Levy, Spectrum Health) Thien Lam, CISO of BayCare Health System, showed the value of outsourced threat detection in real-time to senior management. While everyone was convened, he had his team initiate a ransomware and lock up select machines. His phone rang within 15 minutes, with his vendor reporting the event. "I showed them exactly how fast we can know and react," Lam reported. Buy-in was achieved in real-time.
- **Establishing metrics silos:** "We were having difficulty with consistent apples-to-apples metrics. For example, in our vulnerability scanning, in some areas we get comprehensive information on our credentialed scans, and for others (non-credentialed) we get just basic information. These were originally all lumped together in a risk score, but now we are working to silo them out to keep metrics for groups we get full scans on vs. metrics for groups we get partial scans." (Brad Sanford, Emory University)
- **Weighted metrics:** Though all metrics may be relevant, not all are equal across business threats. "We have metrics around general cybersecurity hygiene health, and then specific metrics that support measurement of executive level cybersecurity risks of interest to our Audit Committee and executives." (Erik Decker, University of Chicago Medicine)
- **Know your audience:** "Be sure to know your audience when reporting out metrics. IT boards and councils are different from senior management, which are different from executive boards. Each is after different information." (Ken Lawonn, CIO of Sharp HealthCare)

SHARP
San Diego's Health Care Leader

"Be sure to know your audience when reporting out metrics. IT boards and councils are different from senior management, which are different from executive boards. Each is after different information."

– **Ken Lawonn**, Senior Vice President and CIO, Sharp HealthCare

"Keep Us Out of the Papers"— Reporting Metrics and Maturity to Boards

"We don't get a lot of guidance and direction from the board in terms of what they want to see," reported one participant, with many heads nodding in agreement.

At Ascension, Bontsas noted, "Board members want the assessment on a scale from 1-10, but the scale keeps changing. Now we may be at a 7, but as soon as we climb to 9, we fall back to 7 as cyber threats continue to evolve and the scale to measure them against changes so quickly. Whatever I report out will change, quickly." Board members tend to have one key top-level concern, he noted: showing up in the newspapers because of a security event. More heads nodded vigorously in agreement from shared experience.

"We can't say definitively that this event won't happen, but we do show what we are doing to prevent that event by focusing on the right things. We report on why we believe we are following the right strategy, and taking the right steps. We show our progress as the threat landscape changes. The board wants a 1-10 measure of assurance, but at the end of the day that is subjective," Bontsas said.

ASCENSION HEALTH

"We can't say definitively that this event won't happen, but we do show what we are doing to prevent that event by focusing on the right things. We report on why we believe we are following the right strategy, and taking the right steps. We show our progress as the threat landscape changes. The board wants a 1-10 measure of assurance, but at the end of the day that is subjective."

– **Jeff Bontsas**, MS, CISSP, Vice President and CISO, Ascension Information Services

TIP: TAKE ADVANTAGE OF NEWS HEADLINES TO EDUCATE. Bontsas takes advantage of board members' interest in news headlines about breaches by using that curiosity—and concern—to educate board members. "At most board meetings, I have five to ten minutes to address what I want to talk about, and the rest is questions about what they've seen in the headlines [or] read in the Wall Street Journal, and how those threats may impact our organization." This speaks to the education gap that is there. "I now regard that Q&A as an important educational opportunity. Ultimately, I believe it will build much more value with our board in the future when we discuss how our strategy and controls will help protect our organization against the threats, risks and breaches experienced by other organizations and governments." Spectrum Health's Lenny Levy added, "Sharing tangible examples of threats detected and mitigated go a lot further than metrics in resonating with leadership and boards."

The Challenge of "Subjective-Objective" Cyber Maturity Levels

While CISOs are regularly asked to assess and weight their cybersecurity maturity levels for their boards or management councils, there are many limitations of maturity assessments—which were broadly regarded around the table as helpful, but ultimately subjective.

Kissinger explained how Banner Health tackled that issue: "For each category in our maturity framework, we've established for ourselves internally that 'to be a 5 means this', and 'to be a 3 it's this.' This is a subjective-objective rating, but we think it's valuable. It shows where we were, where we are today, and where we want to be. I show that I want to move from here to here. This helps us with audit committee and board level discussions."

TIP: BUILD A DOLLAR INVESTMENT/DOLLAR VALUE MODEL TO GUIDE SPENDING AND FUNDING DETERMINATIONS: To complement its maturity framework, Spectrum Health created a framework to show the direct dollar value of its cybersecurity initiatives, and to guide future investments. "To better 'sell' the cybersecurity programs up through our board, we created a framework to illustrate where we are now, what we are targeting and the dollar impact. We worked with actuarial teams from our health-insurer arm to do the calculating to

show business risk, business disruption, direct dollar costs, soft costs and reputational risks. We broke those out," explained Levy. "We built a model to show that as we went from 2 to 3 to 4 to 5 on the maturity scale, we could show how that impacts the curve. For example, if we fund at X level to Y level, we could show investment and benefits. Of course there were many assumptions built in that were well-documented, but with this model we could overlap maturity ratings on a scale and show where we were, where we wanted to go, how much to get there. We could also show spends and the predicted value of the spend."

Lengthy questions followed, given the tremendous interest in Spectrum's model, which Levy has offered to make available (in a desensitized format) to Summit participants and Scottsdale Institute members. CISOs around the table voiced the same desire to get a better handle on not only what an "appropriate" spend is, but how it changes depending on levels of maturity, and how an individual organization spends compared to currently unknown industry benchmarks. While bigger health systems may spend more on cybersecurity than a smaller one spends on total IT, the ratio of spends across maturity levels—and across capital expenditures vs. operating expenditures—is a valuable benchmark to the CISO community.

TIP: REFER TO THE GARTNER GRAPH (Gartner Best Practices for Moving Up the Information Security Maturity Curve) to see a benchmark graphic of levels of spend to get to different levels of maturity.

"From this we could develop and create guideposts more specific to the healthcare sector. This graph that represents the security investments across industries in terms of percent of IT spends and levels of maturity is a good start," said Jim Veline, SVP and CIO at Avera.

EXTERNAL CONSULTANTS AND PEER COMPARISONS IN THE MATURITY ASSESSMENT PROCESS

"When it comes to maturity level, we show our board where we are, where industry is, and how and where we are aiming to grow. We report maturity level progress," said CHRISTUS Health's Blanco, offering a tip that has helped him drive the credibility of his team's maturity assessments: "We now hire an independent organization to do the assessment. After all," Fernando joked, "if I assess myself, I am thinner and taller, so a third-party provides an independent perspective to the board." Many others in the room reported that their organizations were also employing third parties for purposes of objectivity and for an additional layer of credibility to the board on the results.

"We measure ourselves and measure ourselves again, against the same maturity criteria. This works well comparing against ourselves, but comparing to other organizations is where it all falls apart. There is no benchmark to compare to each other, it is subjective even with tools like the Cybersecurity Framework," lamented University of Chicago Medicine's Decker, to broad agreement. Banner Health's Kissinger agreed that peer comparisons were much needed, but woefully lacking. "It would better help us to know how we compare with one another. We and our boards want to know what we are like compared to our peers in the health sector, and in other industries."

Yet, there is also potential downside in comparing across sectors, cautioned Avera's Veline. "We are being held to the same standard as banks. Unfairly. Yet, we in the room are unique

because our #1 business is patient care. While we could look to banking for benchmarking and maturity comparisons, we have to remember that banks aren't buying robotic surgery devices or infusion sets."

Billings Clinic's Thompson drove home shared concerns about the helpfulness of cross-industry comparisons by reminding fellow CISOs about the task their organizations are all focused on at the end of the day: patient care. There are unique challenges in pitting cybersecurity against patient care when it comes to the allocation of dollars and resources at health systems, he opined. "When you pull money away from patient care to put money into a risk that may or may not happen, who wins? Until the system goes down, that is not always clear to leadership—even when we aim to make the business risks and our security impacts clear. Every FTE that I hire or resource that I request is personnel and dollars not going to patient care. So it's a challenge and balance."

CHALLENGE AND BALANCE OF CYBERSECURITY & IT ALIGNMENT

The challenge and balance raised by Thompson also applies to alignment of the cybersecurity function within organization structure and governance. With the increasing visibility of the cybersecurity function and its influence on business risk and impact, many sectors with the same level of complexity of healthcare have moved the cybersecurity function outside of IT. "With large regulated sectors like banking and aerospace, we've seen the security function organized more independently than it is in healthcare. Security has its own budget, leadership role and direct feed to the CEO or board. We don't have that in the healthcare space today, and it's a notable difference," noted Bruce Daly, Deloitte's healthcare digital technology risk leader who co-moderated the Summit. "How many have a security function that has a direct line to the board that could bypass the CIO?" Daly asked. No one responded in the affirmative. This generated a discussion about how to best align cybersecurity and where it could move to in the future.

"We contemplated moving cybersecurity into other places—like reporting to the general counsel or CEO. We ultimately decided that staying under the CIO organization was most helpful in the environment of today, where we need to change many technology elements to bring cybersecurity measures onboard. Once we mature, we can contemplate moving it somewhere else, but for now it is more effective where it is under the CIO," noted Spectrum Health's Levy.

Banner Health's Kissinger said the challenges of appropriate alignment spoke to the "[cybersecurity] row against the [risk] columns." It is the entire organization "that ultimately owns security and cyber-risk challenges, you need deep teaming with IT to be effective today. So embedding with IT is key." Avera's Jim Hanson summed up the discussion by noting that cybersecurity "belongs with the **executive that is most effective in moving it forward.** We could function in several areas, so the issue is not about 'where.' If the executive in charge doesn't

Avera

"Cybersecurity belongs with the executive that is most effective in moving it forward. We could function in several areas, so the issue is not about 'where.' If the executive in charge doesn't have a sense of the function, then it doesn't matter where or how we align in organizational governance."

– **Jim Hanson**, Information Security Officer, Avera Health

have a sense of the function, then it doesn't matter where or how we align in organizational governance."

Better Communications of Business Impact = Earlier Seat at the M&A Table

One of the positive outcomes of better linking cybersecurity to business impact is that it has opened doors for earlier engagement in a key business area notorious for introducing some of the most significant risks and causing the most painful cybersecurity headaches: M&A activity.

"We are noticing nationally a slight but discernable uptick in bringing in security and privacy functions into due diligence for M&A activity," shared Deloitte's Daly. Reaction was quick, with many noting there's much room for growth. Even for those CISOs who are invited to the discussions earlier in the process, many are not convinced that their inputs are carrying weight in decisions.

"I ask a set list of questions I like to ask early and often when it comes to M&A activities," said Banner Health's Kissinger. "At the end of the day, I may not have much influence on a deal even if it is introducing considerable new risks. But at the very least, we are looking for pathways to more visibility in what we are inheriting, so we can get ahead of it and start planning on what we need to remediate."

Banner Health.

"At the end of the day, I may not have much influence on a deal even if it is introducing considerable new risks. But at the very least, we are looking for pathways to more visibility in what we are inheriting, so we can get ahead of it and start planning on what we need to remediate."

– **Bryan Kissinger**, PhD, Vice President and CISO, Banner Health

MOSAIC™ LIFE·CARE

"Mosaic Life Care is bringing in security and risk teams earlier now, including review of contracts. We are getting ahead of things rather than mitigating the risk after the contract has signed."

– **Brenda Williams**, Vice President Technology Services, Mosaic Life Care

Mosaic Life Care is "bringing in security and risk teams earlier now, including review of contracts. We are getting ahead of things rather than mitigating the risk after the contract has been signed," said Brenda Williams, Vice President Technology Services, Mosaic Life Care. "We have introduced it for vendors and we are putting some due diligence in place for acquisitions."

"We are involved before the ink is set. But our access to it is small. We can only ask minimal things. Leadership doesn't want to scare a potential partner with a 300 page questionnaire," one participant shared.

Many opined that even if a review earlier in the process identified clear risk, that likely wouldn't be enough of a red flag to slow down or stop a deal that served other business needs of the company. Often, being at the M&A table was more informative than influential. Deloitte's Daly, however, conveyed a real-world instance when cybersecurity assessments made as part of the diligence process brought real value to an M&A deal he had worked on. "The prospective buyer got a better deal because they had identified some of the core vulnerabilities and risks of the organization they were looking to acquire, and they had calculated remuneration estimates to bring that organization's systems up to speed. They were able to factor this in to an adjusted price. In this way, for smaller-scale acquisitions, early collaboration in the diligence process with security or IT functions can really pay off."

Driving Third-Party Accountability: Vendor Management and Vendor Risks

Similar to the security concerns that M&A introduces are the risks and challenges associated with vendors. Many at the Summit expressed frustration working with vendors who made them feel like they were the "only ones" asking for certain provisions and protections. Many CISOs are also pulling together and standardizing risks and metrics specific to vendors.

To get a better handle on risks posed by vendors, many CISOs are pulling together metrics specific to this area and collecting:

- Percent of critical third parties who have not been risk-assessed
- Percent of vendors who have had security incidents since the last reporting period
- Percent with high residual risk
- Percent of third party system accounts that have not been certified in the last 6 months
- Percent of vendors with high-risk findings
- Percent of vendor X that have not been certified

TIP: GENERATE A HEAT MAP. "We can't fully assess every vendor, but we can generate heat maps with a procurement system or accounts payable overlay," said Emory's Sanford. CISO teams can take a risk-phased approach with that heat map and focus on highest risk vendors.

CALL TO ACTION: Bontsas led a call to action: "As an industry, let's start choosing only those vendors willing to secure their products." These can be generated organization by organization, or preferably, created by associations that can share across the healthcare sector. The National Health Information Sharing & Analysis Center (NH-ISAC) and Medical Device Information Sharing and Analysis Initiative (MDISS) were discussed as a good go-to group to develop such a list. MDISS, it was noted, maintains a large repository of devices and their vulnerability issues, which it shares with members.

Securing Medical Devices with Stronger Vendor Contracts, Micro-Segmentation

Many of the vendor headaches above spill over to medical devices as well, which is already an area of particular concern and risk as it relates to cybersecurity.

"For years we were told by manufacturers that, because the medical devices were FDA approved, we couldn't make any changes or they had to be recertified by FDA. So

relationship with our vendors was tense. We would scan the network, but not these devices. Or similarly, manufacturers would tell us that we could patch devices, but 'if you break something, don't come back to us because it is not the way we configure it. If you patch it, it's your problem,'" recounted CHRISTUS Health's Blanco. The FDA has recently made it clear that hospital systems could patch devices and address security aspects, he said, referencing the 2016 "**Postmarket Management of Cybersecurity in Medical Devices**" guidance to industry from FDA. This led to an around-the-table sharing of other positive experiences leaning on the FDA in related instances, but also to the shared grievances of government punishing businesses for being victimized by cybercrime—which can happen even to the most robust and mature cybersecurity operations.

"Manufacturers tell us 'If you break something, don't come back to us because it is not the way we configure it. If you patch it, it's your problem.'"

– **Fernando Blanco**, Vice President and CISO, CHRISTUS Health

CALL TO ACTION: CONSISTENT LANGUAGE ACROSS CONTRACTS. Blanco reported he has been in touch with Mayo Clinic's CISO, who shared the language it uses in its contracts to hold vendors accountable to the 2016 FDA guidance. "If we all incorporate the language in contracts, we have more power together." **Click here for Mayo Clinic contract**.

TIPS FROM THE TRENCHES/CISO INSIDER INSIGHTS:

> **Micro-segmentation**: Banner Health has been moving to micro-segmentation to secure devices, reported Kissinger. "A lot of security technologies in our server just don't work in clinical devices. So we are doing segmentation and micro-segmentation. Some clinical devices are on their own network, and then infusion pumps, for example, are on their own sub-network segment so that issues can't move laterally across groups of devices."

> **Separate long-term from short-term**: BayCare's Lam noted that as part of his risk planning, he looked at short-term vs. long-term medical device concerns. "We did risk planning to assess what would happen to these medical devices if we had to take down our network. Believe it or not, 90% of the devices we were most concerned about would still function. We identified the few that need to stay on the network, and those that would be okay if the network was down. That helped us establish long-term and short-term protection for our medical devices."

"We did risk planning to assess what would happen to these medical devices if we had to take down our network. Believe it or not, 90% of the devices we were most concerned about would still function. We identified the few that need to stay on the network, and those that would be okay if the network was down. That helped us establish long-term and short-term protection for our medical devices."

– **Thien Lam**, Vice President and CISO, BayCare Health System

- **Overlay patient risk with cyber risk:** CHRISTUS Health is similarly segmenting medical devices by risk, but counseled CISOs not to start with standard patient-safety methodology: "Our first priority when we started this process was infusion pumps and pacemakers, because if these get compromised it has a direct, dangerous impact on patients. What we learned, however, is that these were not the most risky from a cyber point of view. Many did not have wireless capability or were not connected to the network. So these are low-risk from a cyber perspective. We realized we needed to combine patient risk with cyber risk. Now we are reclassifying this risk overlay and identifying new priority devices. We lost a few months on the final deployment based on this risk identification and selection, but now we know how best to deploy," said Blanco. "I hope I can save you a few months with this advice: don't start with standard patient-safety methodology, these were not the most high-risk devices in our current inventory."

- **Align clinical engineering teams within cybersecurity governance**: **"**We have folks installing medical devices on our network who have no IT experience let alone cybersecurity experience. This has been an ongoing challenge that I'm looking to find ways to fix," lamented Christie Polley, System Director, IS Information Security, Eastern Maine Healthcare Systems, noting, "Our supply chain currently handles clinical engineering, with little or no visibility on the IT side." Ascension's Bontsas concurred that with device installation, engineering teams often leave ports and services open and running that are not necessary. "We need to get in front of the implementation so we can have them shut off ports and services that are not needed." BayCare's Lam counseled, "This is something we changed. Clinical engineering now reports to IS and the same CIO. This works really well." Spectrum's Levy added, "We will pull help desk or clinical engineering teams and do exercises together in IT to build relationships so that we can speed coordination in a real-time incident."

EMHS
Access to Quality Healthcare℠

"We have folks installing medical devices on our network who have no IT experience let alone cybersecurity experience. This has been an ongoing challenge that I'm looking to find ways to fix."

– **Christie Polley**, CISM, System Director, IS Information Security, Eastern Maine Healthcare Systems

- **Get manufacturers involved**: "Over the long term, we have to get the manufacturers on board to work with us," said Lam, with much agreement from the table. The need for more manufacturer cooperation, particularly for patches for "end of life" devices and equipment, was emphasized. While the enhanced contract language referenced above will help moving forward to hold manufacturers accountable for updates and patches, participants recognized the near-term challenge is the legacy systems in place that have no contract terms to make vendors more accountable.

- **Work together on standard demands**: "We regularly get push back from vendors when they say we are the 'only ones' asking for certain protective measures and contract terms. We need the ability to reach out to others so that we can standardize our demands and 'asks'," said BayCare's Lam. Summit participants also planned, as follow-up, to build a better mutual understanding regarding how and when CISOs are reaching out to the FDA.

Cybersecurity Training: It is Everyone's Business to Protect the Business

Ultimately, it is everybody's business to protect the business from cybersecurity risks—which spills over to the need for training staff across the organization. Yet, participation in and compliance with training is a frustration shared across CISOs at the Summit. Discussion focused both on the "carrot" and the "stick"—on how CISOs were attempting to make it easier for providers and health system staff to complete training, and how discipline and sanctions were being put in place for those who were non-compliant.

TIPS FROM THE TRENCHES/CISO INSIDER INSIGHTS:

- **Provide context:** "We made a two-minute video explaining to new hires the importance of cybersecurity and their role in it. Then they have a mandatory training module to complete online within 15 days of onboarding, but at least with the video they now have the proper context and motivation to complete the training." (Fernando Blanco, CHRISTUS Health)
- **Make it real:** "Members of my team and I started personally going to senior staff meetings and getting on agendas each quarter. We talk briefly about threats and risks and provide tips. We made cybersecurity more real and personal rather than something that simply emanates from corporate. We've gotten great feedback about that." (Bryan Kissinger, Banner Health)
- **Set a consistent calendar of training expectations:** "We launch interactive educational modules a minimum of 4x year, along with our bi-monthly reminder communications. We struggled at first with pushback on that frequency, but we have taken a stand." (Christie Polley, EMHS)
- **Enable, rather than only restrict:** "We have tools that we have certified for employees to use, for example, the file-sharing tool box. That way, we weren't just putting out restrictions to tools like Dropbox and Google Drive, we were also providing an alternative." (Brad Sanford, Emory University)
- **Align training to safer computers at home:** "Our biggest successes in terms of staff engagement come not from a 'how to be secure at work' approach, but from training and communications focused on how to be more secure online at home. People were very motivated when it came to their home computers and emails, and we realized we could offer advice there that can then bleed back over into work." (Lenny Levy, Spectrum Health)
- **Be prepared for paradoxes:** "We did some internal testing, and what we learned showed a training paradox. Our healthcare division performed much worse in phishing tests but had a nearly 100% completion rate in training; our university staff performed better on the phishing tests, but were much less compliant in training." (Brad Sanford, Emory University)

With regard to how to discipline or sanction a provider who is adding benefit to the organization from a patient-care perspective, but who hasn't been compliant with training, CISOs have taken a variety of approaches. Some have made noncompliant providers ineligible for a pay raise. Others reported they have in fact terminated people based on long-term noncompliance. One

creative solution being considered is a quarterly report, entered into board minutes, that lists all employees who have completed cybersecurity trainings…and all who have not. The thinking underlying this approach: being named on a noncompliance list will be frightening to providers, and that alone could be motivation to complete training. At the end of the day, CISOs agreed, sanctions and discipline must be set as part of an organizational culture discussion, and must have the buy-in of leadership.

Conclusion: The Tail Will Wag the Dog

Even with its challenges and frustrations, CISOs have come a long way for a role that barely existed in healthcare organizations a decade ago. With the realization that security breaches can derail profits, damage reputations and ultimately hurt patient care, health systems are now moving toward enterprise risk management (ERM). CISOs are well poised to play an active role in that evolution, and in many ways, can be the proverbial tail that wags the dog when it comes to understanding, assessing and managing risks and threats across an organization. After all, that has been a focus we have been pushing up and out on the cyber front for years. With the evolution to ERM, the imperative to understand and articulate risks/threats within the context of business impacts will only increase.

> *"We started rolling out annual risk review process, doing portions of it across the entire year to have completeness across the enterprise. However, we do not have a formal ERM process, so we in the cybersecurity function are currently the tail wagging the dog as we implement continuing monitoring and continuous assessment."*
>
> – **Lenny Levy**, Spectrum Health

> *"We are just now working on moving towards a true ERM process at EMHS with our general counsel's office leading the charge. Our security department is much further along in the process of how to identify and report on security risk than the system seems to be with overall risk, so we are helping them understand how it works."*
>
> – **Christie Polley**, EMHS

Indeed, our current role as a "row within columns" may in fact be the jumping-off point as we guide health systems through ERM adoption over the next five to 10 years. Our experiences, challenges and frustrations today may in fact be the fodder that guarantees us a seat at the table tomorrow.

About the sponsors

The ***Scottsdale Institute (SI)*** is a not-for-profit membership organization of prominent healthcare systems whose goal is to support our members as they move forward to achieve clinical integration and transformation through information technology.

SI facilitates knowledge sharing by providing intimate and informal forums that embrace SI's "Three Pillars:"

- Collaboration
- Education
- Networking

For more information visit:
www.scottsdaleinstitute.org

SCOTTSDALE INSTITUTE
COLLABORATION • EDUCATION • NETWORKING

About 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:
www.deloitte.com/us/providers

Deloitte.

Icons designed by Vexels.com