CISOs

SCOTTSDALE INSTITUTE 2018
CHIEF INFORMATION SECURITY OFFICERS

CYBER RISK STRATEGY FOR THE FUTURE

September 26–27, 2018 | Chicago, IL

SCOTTSDALE INSTITUTE
COLLABORATION • EDUCATION • NETWORKING

Sponsored by:

Deloitte.

Executive Summary

Fifteen Chief Security Officers (CISOs) of leading health systems convened in Chicago in late September to discuss key challenges and best practice standards in healthcare cybersecurity today. During the two-day meeting, they focused on managing third-party risk, medical device security, recruiting and retaining personnel, and their role within the organization. This report captures their discussion and shared insights.

Summit Participants

Fernando Blanco, VP & CISO, CHRISTUS Health

Dan Bowden, VP & CISO, Sentara Healthcare

Chris Convey, VP & CISO, Sharp HealthCare

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

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

Scott Dresen, SVP & CTO/CISO, Spectrum Health

Michael Erickson, CISO, Baptist Health

Jim Hanson, Regional Information Security Officer, Avera Health

Preston Jennings, VP Information Security & CISO, Trinity Health

Bryan Kissinger, PhD, VP & CISO, and Interim CIO, Banner Health

Thien Lam, VP & CISO, BayCare Health System

Paul McAninch, Director IS & Compliance, IU Health

Bryan McDowell, CISO, University Hospitals

Paul VanAmerongen, VP & CISO, UW Health

Russ Walker, VP & CISO, Adventist Health System

Convener: Scottsdale Institute

Chuck Appleby
Janet Guptill, FACHE
Cindy Mendel
Gordon Rohweder
Cynthia Schroers

Sponsor: Deloitte

Anand Dedhia
Shari Gribbin
Unna Narayanan

Writer: Debra Gordon

Moderator: Raj Mehta, Deloitte

Introduction

Raj Mehta, Cyber Risk Services partner with Deloitte Advisory, moderated the CISO Summit discussion, guiding participants through a series of questions and topics designed to garner their experiences and opinions on current cybersecurity-related challenges in their organizations.

Setting the stage for the give-and-take, participants were given an insider's view of the most important government initiative in healthcare cybersecurity today.

UPDATE ON 405(D) NATIONAL CYBERSECURITY WORKING GROUP TASK GROUP

Erik Decker, Chief Information Security and Privacy Officer at University of Chicago Medicine and industry lead on the task group, presented an overview of the 405(d) task group, created as part of the Cybersecurity Sharing Act (CSA) of 2015. Section 405(d) of the Act, Aligning Health Care Industry Security Approaches, requires development of consensus-based guidelines, best practices and methodologies to strengthen the healthcare and public-health sector's cybersecurity posture.

In May of 2017, the Department of Health and Human Services (HHS) convened the task group, which includes more than 150 information security officers, medical professionals, privacy experts and industry leaders. The group has spent the past 18 months developing a targeted set of applicable and voluntary guidance measures to cost-effectively reduce the cybersecurity risks of healthcare providers.

"We are trying to move the cybersecurity needle across the industry," Decker said. "We're not trying to solve all the problems, but focus on the threats we all face and the most impactful cybersecurity practices we could implement to mitigate these threats."

The task group's guidance, due to be released by the end of the year, identifies five key threats to the industry and 10 cybersecurity practices that could mitigate those threats based on the size of the organization, he noted. The report includes a toolkit that allows organizations to prioritize their threats, which will dynamically provide a recommended priority of cybersecurity practices to implement. It also helps organizations evaluate their current state and help set a target state. This effort has been aligned and mapped to the NIST Cybersecurity Framework.

> "We are trying to move the cybersecurity needle across the industry. We're not trying to solve all the problems, but focus on the threats we all face and the most impactful cybersecurity practices we could implement to mitigate these threats."
>
> – **Erik Decker**, Chief Information Security & Privacy Officer, University of Chicago Medicine

"This is not a new regulation or a checklist," said Decker. Instead, the intent is to assess the vulnerability of an organization to the five threats—or others, if necessary—and identify the most impactful processes to mitigate those threats. "It's a voluntary tool that will help organizations tackle these modern cybersecurity challenges" he said.

While the guidance is nearly finished, the task group is charged with continually updating this guidance. This is a fantastic way for other CISOs to get involved, Decker said, and he strongly encouraged everyone there to take an active role in any of the related efforts of the **Healthcare Sector Coordinating Council Joint Cyber Working Group.**

405(d) Task Group Goals

The task group is charged with developing a common set of voluntary, consensus-based and industry-led guidelines, best practices, methodologies, procedures and processes that:

- Serve as a resource for cost-effectively reducing cybersecurity risks for a range of healthcare organizations;
- Support voluntary adoption and implementation efforts to improve safeguards to address cybersecurity threats;
- Are consistent with existing laws and regulations, including the National Institute of Standards and Technology Act; the Health Insurance Portability and Accountability Act of 1996; and the Health Information Technology for Economic and Clinical Health Act;
- Are updated on a regular basis and applicable to a range of healthcare organizations.

THIRD-PARTY RISK MANAGEMENT

Third-party risk management is a consistent concern for healthcare organizations given a growing dependence on such vendors. However, a global study from Deloitte found few organizations are capable of managing the risks of third parties, with just 20.1 percent reporting they have integrated or optimized their third-party governance risk management (TPGRM) mechanisms.[1]

"Everybody is, to a certain extent, doing TPGRM as part of the procurement process," Mehta said. But should organizations be doing more, he asked, including proactive assessments and leveraging shared assessments?

With that, Mehta opened the floor for a robust discussion about the challenges and processes the participating CISOs face when it comes to third-party risk management.

At Memorial Sloan Kettering Cancer Center, cybersecurity participates in the request for proposal process and provides an assessment of the potential security risk posed by the products and/or service, said Vice President and CISO Mike Czumak. "Sometimes it influences the business decision, but it's not the only decision point," he said. "We have to weigh the business piece with the security piece. But we're up front and say, 'If you go with this vendor, here are the risks we see based on their responses that you'll have to address sooner or later.'"

Best Practices

The discussion around third-party risk management elicited numerous examples of best practices.

Streamline the assessment questionnaire

When Bryan McDowell, CISO at University Hospitals, received a third-party risk assessment questionnaire from Google, he was shocked to find just five questions. "I'm used to 217 questions," he said. "But it was clear that the questions were well thought out and would provide the information Google needed to know if it wanted to do business with UH." Impressed with the quality and brevity of the questionnaire, McDowell developed his own short list of 23 questions for UH's vendors, and offered to share it with other participants.

Get the lawyers involved

Czumak recently added an attorney to his team for contract review. He also has five people who focus just on security assessments and penetration security testing for third parties. "Quite often we don't get a full assessment done prior to contract, just because we want to actually get hands on and test the final product," he said. So they now build language into the contract requiring the vendor to fix any vulnerabilities later identified within a certain amount of time.

Test all vendors

Memorial Sloan Kettering tests all its third-party vendors, said Czumak, even the large ones. "We build it into our contract," he said, even though it might extend negotiations. They also accept third-party penetration tests as long as they can review the methodology; the methodology aligns with their own processes; and they are given insight into the results.

Then, "when we do an initial up-front test, it's typically just to validate certain technical controls," Czumak noted. To supplement those point-in-time tests, his team also engages with the vendors directly to gain as much understanding as possible about their processes and ability to share security information. Those conversations provide a lot of useful details and they can quickly uncover whether the vendor truly has invested in its security practices. "I just want a gut feel that they know what they're doing, and they've got some program in place," he said.

Monitor vendors

Participants described monitoring major vendors from network media to the Dark Web, and sometimes finding hacked data. "It's not a weekly thing that we're finding stuff," said Czumak, "it's just another control in place to make sure you're staying on top of everything." Some participants are outsourcing such tracking to companies like Flashpoint, which provides contextual intelligence.

"I'm used to 217 questions. But it was clear that the questions were well thought out and would provide the information Google needed to know if it wanted to do business with UH."

– **Bryan McDowell**, CISO, University Hospitals

Make site visits

Some CISOs said they ask for site visits. "If a vendor balks at this, I would question that," said Dan Bowden, Vice President and CISO at Sentara Healthcare. "If they act evasive, that's a huge red flag."

Build internal relationships

One important component of third-party risk management is building internal relationships with key individuals in other departments who, during technology deployment, can ensure that information security is involved. For instance, Bowden sits on Sentara's Information Technology Review Board, which tracks new technology that may come out of business and clinical trials. Nonetheless, he said, quite a lot flies under the radar, particularly when providers move in from other institutions and bring their own equipment.

Keep the reports relevant

At Memorial Sloan Kettering, the risk review, acceptance and mitigation documentation provided to the executive owners of the RFP includes a section that explains what it means. "We've developed standardized business-related language, executive-owner style language around every finding that we have in our catalogue that puts it in plain English," said Czumak. Basically, the report is designed to answer the questions: What does this mean and what risk does it pose?

The health system also requires that business representatives articulate the business risk of *not* engaging the vendor, or delaying the engagement.

Involve vendors in disaster exercises

Several participants involve critical vendors in tabletop security exercises as part of their third-party risk management strategy. They also stress building cybersecurity into any disaster plan and ensuring that vendors respond appropriately during an emergency.

Participants described a variety of tools they use for assessing third-party vendors, including BitSight and RiskRecon for scoring vendors, and CORL to analyze and manage the risk environment. Several also outsource assessments.

Capturing the data necessary to conduct third-party risk analysis can be an exhaustive process," said Decker. His organization outsources the information-gathering process then has internal analysts review the results. They ensure all supply-chain contracts undergo risk evaluation and track the average risk grades of new vendors on a monthly basis. Leadership reviews the average risk postures as part of their standard cybersecurity risk-governance practices.

One challenge is determining how to handle legacy contracts. "We are trying to determine who are our biggest vendors that haven't come up for review because their products have been here forever?" asked Paul VanAmerongen, Vice President and CISO for UW Health at the University of Wisconsin. His company sent a questionnaire to 10 such vendors. "Some of the responses were shocking," he said.

It's easier to require security assessments for on-premise technology implementations, as opposed to cloud solutions, because IT involvement is often required for deployment. Given the increasing appetite for organizations to go cloud, it's critical they have ways to prevent

its unsanctioned usage, said Sharp HealthCare Vice President and Chief Information Security Officer Chris Convey.

"It's easier to require security assessments for on-premise technology implementations, as opposed to cloud solutions, because IT involvement is often required for deployment. Given the increasing appetite for organizations to go cloud, it's critical they have ways to prevent its unsanctioned usage."

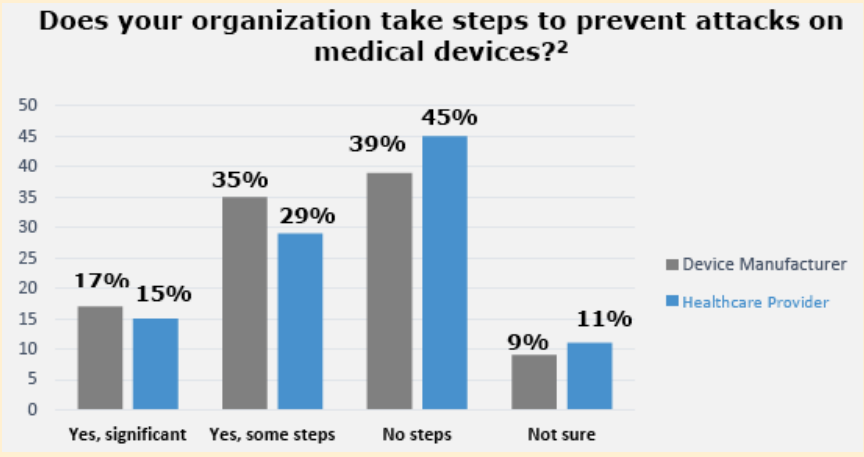
– **Chris Convey**, VP & CISO, Sharp HealthCare

MEDICAL DEVICE SECURITY: THE INTERNET OF THINGS

The Internet of Things (IoT) is transforming healthcare from the hospital setting to the home. Apps, smart wearables, implantable devices, monitoring equipment—all are collecting, analyzing, and storing terabytes of data that can improve healthcare delivery and reduce costs. They also represent one of the greatest security vulnerabilities in the field, particularly when it comes to medical devices.[2]

According to a survey from the Ponemon Institute, 67 percent of the 242 individuals surveyed who worked for device manufacturers believed an attack on one or more medical devices their company built is likely and 56 percent of a similar number of healthcare-delivery organizations (HDOs) believe such an attack is likely. Yet just 17 percent of device makers and 15 percent of HDOs were taking significant steps to prevent attacks, with just 22 percent of HDOs and 41 percent of device makers saying their organizations have an incident-response plan in place in the event of an attack on vulnerable medical devices (Figure 1).[3] Numerous attacks have already occurred, putting patients at risk.

FIGURE 1



Source: Ponemon Institute. Medical Device Security: An Industry Under Attack and Unprepared to Defend. May 2017. Available at: https://www.synopsys.com/content/dam/synopsys/sig-assets/reports/medical-device-security-ponemon-synopsys.pdf

In one survey, 29 percent of respondents thought the CISO should be responsible for ensuring IoT security.[4]

"What are your organizations doing from the medical device perspective?" Mehta asked. Most participants responded with frustration at both vendors who don't take security seriously enough and internal customers who don't understand the risks.

"Most surveillance tools don't identify devices (on the network) in enough detail to be helpful."

– **Paul McAninch**, Director IS & Compliance,, IU Health

A major challenge, said Preston Jennings, Vice President Information Security and CISO, Trinity Health, is the "unmanageable device," one that's unpatchable, can't be configured and can't be accessed. "Yet you have to figure out how to effectively deliver and secure it within your environment, in real time with, in most instances, no direct authority over the device itself."

In addition, noted IU Health Director of Information Security and Compliance Paul McAninch, "most surveillance tools don't identify devices (on the network) in enough detail to be helpful."

"Providers have an obligation and liability for ensuring the safe and effective use of these devices in patient care," Decker said, yet some vendors insist on implementing these devices by leveraging their own practices (such as installing their own firewalls and remote access systems). "When a vendor deploys in this manner, the providers lose visibility." This approach poses a big risk. "What if a vendor we all use gets compromised, and these remote access solutions are used to access not just one provider but multiple providers at the same time? What if they are connected to surgical robots or a linear accelerator?" he asked. "I think it's very important for us to collectively think about this risk with the context of threat actors that might be interested in causing regional cyber attacks."

Those risks are only growing, participants agreed. "You have a 10-year-old terminally ill cancer patient and all he wants to do is play the Xbox," said Jennings. "So how do you *not* bring in an Xbox and put it on your network and allow that kid to play Fortnite? The reality is that Amazon Echoes are coming, we're going to have Apple TVs everywhere, we've got IP cameras and HVACs that are not under IT, and we've got to figure out solutions to allow these to live in our environment, to know where they are, to know what they're talking to, and then to minimize risk around driving traffic to and from these devices."

"Organizations need to work together as part of their group purchasing organizations to force device vendors to include standard contract language that addresses security."

--- **Preston Jennings**, Vice President, Information Security & CISO, Trinity Health

One concern, said Jennings, is that the Food and Drug Administration (FDA) may start requiring patched, secured operating systems and platforms for all devices, which could lead to vendors ending their support of aging software. "What if the vendor turns around and says the linear accelerator you're planning on using for 10 years is running Windows 7 and we're ending support?" he asked. "Then you have to buy another linear accelerator after just six years."

However, noted Decker, Congress is bringing vendors to the table to talk about life cycle and legacy support given these aging operating systems.

Vendors don't provide enough support now, asserted participants. "It's like chipping away at this huge glacier" to get vendors to update equipment, said Czumak. "We do full assessments like we would any technology, but then we get into the real details where I have to spend weeks on the phone with one vendor asking why they aren't updating the software, why there is no auditing or authentication? They say, 'Well, this is our six-year plan, or no one else is asking for this, or the FDA says we can't do this.' So, it's kind of like chasing your tail."

> "It's like chipping away at this huge glacier" to get vendors to update equipment. "We do full assessments like we would any technology, but then we get into the real details where I have to spend weeks on the phone with one vendor asking why they aren't updating the software, why there is no auditing or authentication?"

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

"We discovered when looking at some medical-device support contracts that we're paying for nothing but reactive responses when problems arise, but nothing is included that requires proactive patching by the vendor," said Scott Dresen, Senior Vice President and CTO/CISO at Spectrum Health.

Best Practices

- Ask for vendors' audit reports to know who's accessing the system.
- Conduct a weekly report to track segmented devices versus those deployed incorrectly on the general access network.
- Implement more robust upfront-assessment processes when procuring medical devices based on risk.
- Procure skill sets with clinical engineering and cyber-security background.
- Implement robust risk-management processes for managing life cycle of risks and reporting.
- Implement medical-device security-monitoring tools and integrate monitoring and incident-response processes with the Security Operations Center.

Finding and Retaining Talent

With a cybersecurity unemployment rate at zero, more than 1.5 million openings expected by 2019 in the field, and 84 percent of cybersecurity workers in 2018 saying they're open to new opportunities or already planning a job search, recruiting and retaining talent has become a huge challenge in the industry.[5,6] Yet cybersecurity departments, like all areas of healthcare, are being tasked to do more with less.

"So how do we grow, optimize and retain the right talent?" Mehta asked. "How do you get more out of your workforce?" added Shari Gribbin, Senior Manager, Cyber Business & Operational Risk, Deloitte.

You have to create a culture that challenges and rewards employees, said Russ Walker, Vice President and CISO, Adventist Health System. "Technical people are very curious. They want to learn and grow, so you have to create career paths for them based on their interests." He helps his employees create a career path then rotates them through various parts of the organization.

"This does two huge things," Walker said. "It gives them more tools in their tool belt and prepares them for their next job by exposing them to different disciplines. It also means that we can develop very deep bench strength and eliminate single points of failure."

He believes strongly in empowering individuals to make a strong team. "When I promote people, I make a very big deal about why I promoted that person. I want everyone to understand that the person who got promoted has a passion to learn, that they are willing to share their knowledge, they're willing to grow the people around themselves, and they are team players. That's the culture I've been trying to build and I think I've been very successful at it."

> "Technical people are very curious. They want to learn and grow, so you have to create career paths for them based on their interests."
>
> – **Russ Walker**, VP & CISO, Adventist Health System

When he first arrived at Banner, Bryan Kissinger, Vice President and CISO, Banner Health said, there were only a handful of position levels in his department: analyst, consultant and director, which made it difficult to retain talent because it took so long for people to advance. "If you think you're going to hold on to a security analyst you trained for five years without them jumping to get a promotion, you're crazy," he said. To address the problem, he is working with human resources to create intermediate steps between those positions, such as senior analyst.

McDowell had the opposite problem. His team had become quite top heavy. Now he is working with human resources to split some senior jobs into two lower-level jobs. "My justification is that, including benefits, it's a net $30,000 difference to my budget. But if I create a couple of

level-one or level-two employees, instead of having a top-heavy senior technical resource, I can try to grow them."

At UW Health, VanAmerongen is experimenting with building a competency-based program within information security based on the person's skill set and qualities versus their years of experience. "You can't require 14 years of experience in technology," he said, particularly in security. "You often want the guy out of college who has no work experience at all to lead a new and innovative program."

> "Folks in this industry, they're competitive, they like to get promoted, they really are interested in moving up."
>
> 
>
> – **Bryan Kissinger**, VP & CISO, and Interim CIO, Banner Health

It's also important to consider what stage people are in their lives, said Walker. "For example, I have a woman who was really sharp, but she just didn't have the time to put in the extra effort at work because she had two young children at home. But as her children grew up, she was able to put more and more time into work and when the kids were 9 or 10-years old, she took off like a rocket." In the early stages, however, "we wanted to accommodate her and understood she couldn't take on certain projects because of her limited time. The takeaway here is that people's needs and interests are constantly changing and you have to understand that," he said.

Participants also discussed the growing number of people now graduating with degrees in cybersecurity, something that didn't exist when they started in the field. "We're some of the last of a breed here," said VanAmerongen. However, the degree doesn't necessarily make them the best. "From my experience, I want to get the people who came out of infrastructure, who came out of applications, who came out of the customer-service help desk. I want those experiences on my team," he said. "I can teach them about security and build it up that way." Those coming out of the training programs, he and others noted, have a concept of security that is basically "lock it down and shut it off," which isn't advisable in healthcare.

"The good thing is the more you grow your people, the more excited they get about working for you and the less likely they are to leave," said Walker.

> "We're some of the last of a breed here. From my experience, I want to get the people who came out of infrastructure, who came out of applications, who came out of the customer-service help desk. I want those experiences on my team."
>
> – **Paul VanAmerongen**, VP & CISO, UW Health

The Intern Pipeline

The idea of using interns captured the group's attention. Banner Health has a robust internship program. At $12.50 an hour, Kissinger said, the local university students provide exceptional value as well as a built-in recruiting pipeline. "We had an employee who unexpectedly resigned, and we had an intern everybody liked, so we didn't even need to do any recruiting. We just moved this guy who was graduating in a couple of months into the full-time role and moved on with our lives."

> "What's interesting about the students is that a lot of them had never contemplated a career in healthcare IT, let alone cybersecurity."
>
> – **Scott Dresen**, SVP & CTO/CISO, Spectrum Health

Dresen also runs a robust internship program at Spectrum Health that has become an important part of their hiring pipeline with a greater-than-50-percent conversion rate. "What's interesting about the students is that a lot of them had never contemplated a career in healthcare IT, let alone cybersecurity," he said.

At Sentara, about a dozen interns work part-time and several have been hired for full-time positions. "The point is to create that pipeline, right?" said Bowden. Even when the interns take jobs with other companies, it shows their talent. "If you have a 20-year-old kid, he's just going into his junior year, survived the interview process and got an information-security job at a major health-insurance payer, then I tell his boss: 'You're a rock star manager and leader,' " he said.

Bowden recommended talking to local universities, many of which are applying for NIST and state technology grants to support the development of STEM students. Some will even reimburse part of the intern's salary.

"We've built a profile of the best person for the job," he said. "For instance, for governance, risk and compliance, writing and analytics, we know the best person is an older student, such as a veteran in her or his mid-20s who is returning to college." They tend to have more analytical skills and previous job experience, he said. Those with white-hat hacking experience tend to do better as junior SecOps.

The students are extremely valuable, he said. "I think a lot of people look at students as a babysitting job. If that's how it ends up, then you don't know how to pick the right person." For instance, during a spear-phishing attack, "I walked downstairs and there's me and three managers standing and leaning against the wall watching the students deal with it." The students also manage daily assurance checklists, he said, "and they know nobody goes home until these assurance things are all checked off."

Basically, he said, the interns (who include graduate students) now run most of the SPAM and anti-phishing the programs themselves.

"[The interns] bring value to the team. We miss them when they're not there."

– **Dan Bowden**, VP & CISO, Sentara Healthcare

Overcoming Environmental Obstacles

Market size can be a challenge when it comes to recruiting, said Dresen. "In a market the size of Grand Rapids, we have the difficulty of a smaller talent pool to draw from for our talent, and the attraction of larger markets pulls our people away."

One way to overcome geographical challenges is to hire remote employees. "My boss wanted to hire everybody in Orlando," said Walker. "I told him that I wouldn't find the talent in Orlando, and a lot of people don't want to move to Orlando." After six months of searching, he found two "rock stars," both of whom lived in Nashville and didn't want to relocate. He was able to hire them with the understanding that they would come into the office one week per month. "This has worked incredibly well. At the moment, I've got people in Denver, Houston, Virginia, Nashville, all over the place."

"I would say probably 60 percent of my team lives in markets where we don't have facilities," said one CISO. He's currently hiring team members to work remotely and installing a virtual Security Operations Center (SOC) in their home at a cost of about $3,500 per individual instead of the traditional on-premise SOC that can run upwards of a million dollars.

While remote employees can be challenging, said Walker, one way to gauge their productivity is with a ticketing system. "The other indicator is that when I call somebody and they respond immediately and are on their computer, I know they're sitting in front of the computer." Sometimes people abuse the privilege, he said. "One woman who worked for me thought it would be a great idea to work out of her Starbucks. But her productivity suffered and as soon as we identified this, she lost her privileges and eventually her job."

One challenge with remote employees, said McDowell, is that the salary range is based on the home market, not the employee's market. "It's really hard to have somebody working where they want to live and it's in a higher cost-of-living area," he said. He is working with his human resources department to review compensation for IT security positions on a national versus a local level.

Salary Structure

No matter how motivating the culture, salary still plays a major role in recruitment and retention.

For instance, it's important that human resources understand the difference between what information security professionals are paid in the broader market versus within hospitals, which could lead to lower salaries and make recruitment more difficult.

"If you're not keeping the salaries within 10 percent of market rates you're not going to keep the people," said Walker.

Closing the Deal

The interview process is also important, said Jennings. That means showing applicants the passion behind security and what you're building. "People will take a pay cut so they can come to a team where they're engaged, where they have a voice, where they're helping to build something," he said. That's a big differentiator for healthcare. To that end, when he's interviewing, he talks about the company's mission, its commitment to the community. "People get excited about that."

McDowell agreed. "We spend so much time standing on the digital-fort walls staring into the abyss of everything that's coming at us, we rarely turn around to see why we're doing it, which is the great work the physicians and caregivers are doing to treat patients. I walk through the children's hospital on a regular basis to remind myself that we're protecting the data of these patients and people in vulnerable states, as well as keeping the systems online to allow our caregivers to provide the best treatment. This is why I come to work every day."

Thien Lam, VP & CISO, BayCare Health System

Jennings cited humility as a strategic virtue. "Find people who are smarter than you. Embrace those people, bring them in. They're coming in to give you information you don't have so you can make better decisions," said Jennings.

Walker said, "I've told my people there are no artificial barriers. Your experience is not an issue. I'm looking at performance. If you work hard and you can do the job, you're going to get the job, irrespective of experience, age, sex or the color of your skin."

Using Automation to Improve Productivity

In a world in which teams are being stressed to do more with less, Mehta asked, "is anyone applying automation to deal with certain tasks and thus offset staff time?"

Several participants said processes such as robotic process automation (RPA) for phishing email responses can free up employees for more complex tasks. Outsourcing managed security services (MSS) for tier-one responses as well as content development can also reduce costs and improve productivity as long as the internal team understands the role of the MSS team and learns to work closely with them.

DevOps, which integrates coding with security throughout the software-development process, so it can be automated as part of the CI/CD chain testing, can also improve productivity and security features. "It's greatly improving our ability to mitigate risk as software is being developed rather than after the fact," said Dresen. As developers promote their code through the development cycle, integrated security tools scan the code to identify insecure coding practices and block the code from being promoted until the identified issues are resolved.

Best Practice

One CISO participant tracks the dollar efficiency of his organizational gains by automating and reporting it to executive leadership. His team also practices lean management, highlighting areas for improvement throughout the organization.

From the Trenches

Throughout the discussion on recruitment and retention, participants highlighted several successful approaches:

- **Make quick decisions.** "One of my directors has the offer letter lined up before the interview so he's ready to make an offer," said Jennings.
- **Fire people who are not performing.** "Otherwise, it drags down the morale of the teams," said Walker. "If you do not fire them, you will lose the respect of the other employees."
- **Hire ex-military.** "They're very structured, they know how to take orders, and they don't have this incredible sense of entitlement," Walker said.
- **Survey the team.** Participants used tools such as Press Ganey scores and POPin, an anonymous crowdsourcing tool, to get feedback from employees. "It's been really good for engagement," said Kissinger. "Whether it's a voice survey or some sort of other engagement tool, providing that forum for your teams to hear from you directly is important." When he receives annual employee-survey results, he asks the team to identify solutions to the problems. Then they regularly review progress and results.
- **Encourage entrepreneurship.** One member allows team members to spend 10 percent of their time on their own research and development.
- **Recruit from within.** Some of the best people come from other parts of IT, said Kissinger. "It's great because they bring a lot of intellectual property and knowledge with them, they want to learn security and they know a lot of people."

The CISO as Business Advisor

Where does the CISO fit within the greater organization? How do they lead beyond security? Those were some of the issues participants wrestled with during the next part of the discussion as Mehta charged them with assessing their role as a business advisor.

He highlighted four main roles of the CISO he observes when talking with CISOs around the country: (Figure 2):

- Strategist: Connecting with the business side of the organization and focusing on the future;
- Advisor: Guiding the organization in areas around risk;
- Guardian: Developing and implementing policies and procedures;
- Technologist: Understanding the technology required for success.

CISOs who are promoted tend to spend more time as strategists and advisors, he said. "That's something to think about in terms of how you spend your time and how you can elevate your influence across the organization."

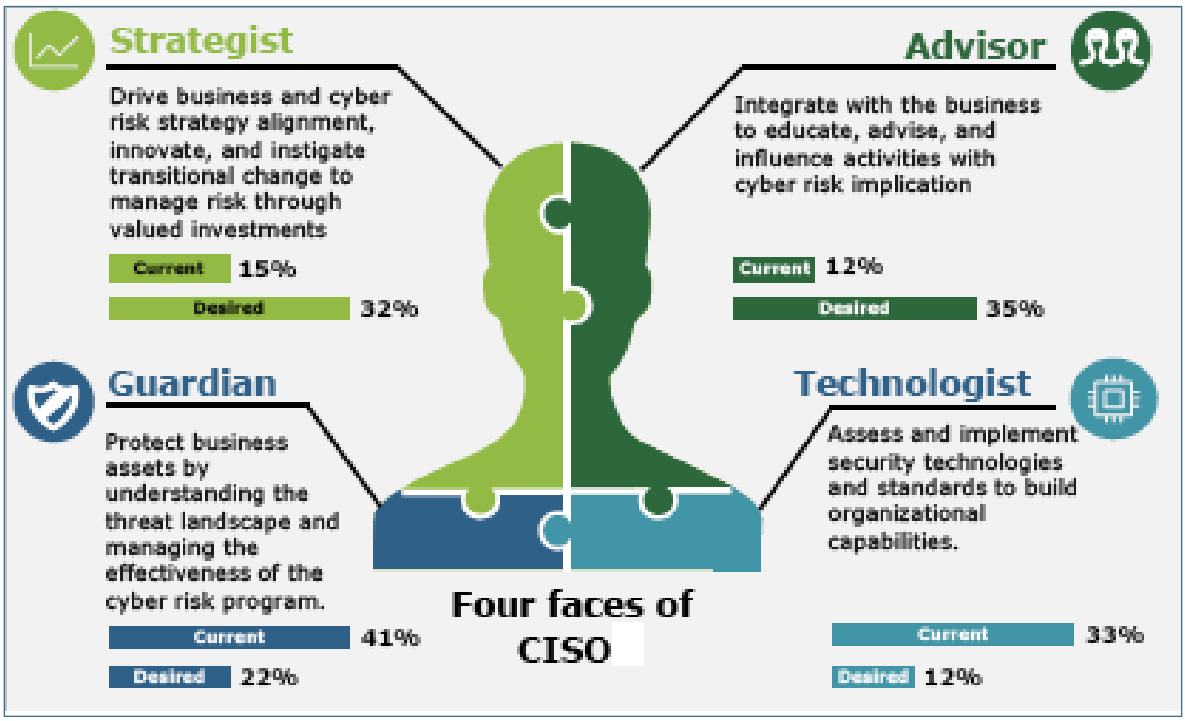
Michael Erickson, CISO of Baptist Health, agreed with the assessment. The CISO role is not to block initiatives or solely focus on loss-avoidance activities, he said. "It's about reducing friction to enable the business to move faster. To expand the view of our role, we need to align our efforts to strategic business goals and demonstrate value in business conversations by helping our organizations thrive."

> "It's about reducing friction to enable the business to move faster. To expand the view of our role, we need to align our efforts to strategic business goals and demonstrate value in business conversations by helping our organizations thrive."
>
> – **Michael Erickson**, CISO, Baptist Health

"We have to play bigger," asserted Kissinger. "We need more opportunities to be business leaders, not security or IT leaders. That to me is the most important thing in creating a career path."

At IU Health, McAninch noted, his department is pursuing selling "CISO as a Service" to the broader university.

FIGURE 2 THE MODERN CHIEF INFORMATION SECURITY OFFICER



The Rounding CISO

Several participants cited the importance of organization-wide interactions to demonstrate the relevance of security and build their brand within the system. Such internal support, they said, can help overcome "blockers" who may impede progress.

Kissinger has made it a mission to visit hospitals in the six states in which Banner operates, including rural hospitals and facilities, something he calls "rounding." "Every person I talk to, I learn something new about what they think about security or what they think about IT or what they're challenged with," he said. The result: enhanced relationships with the business owners at the hospitals. "We have to get out there and meet with them and invest that time. These efforts are priceless," he said. At Sentara, the CIO to whom Bowden reports just added a business-relationship management processes (BRM) team that goes into the field and talks to people throughout the organization. "What's cool is they can bring information back to us and we can funnel information out through them," Bowden said. "It's already a huge home run because I have exposure and visibility to things that I had no idea about before."

Jim Hanson, Regional Information Security Officer, Avera Health agreed: "I routinely meet with executives at Avera facilities all across the region, and that 'windshield time' is an invaluable investment of my time."

> "I routinely meet with executives at Avera facilities all across the region, and that 'windshield time' is an invaluable investment of my time."
>
> – **Jim Hanson**, Regional Information Security Officer, Avera Health

Decker got that opportunity recently when the CFO at University of Chicago Medicine announced its first enterprise risk-management program and asked information security to be the first department to present to the Board. He worked for months with the CFO to develop enterprise methodologies.

"I showed them the plot from where we were three years ago to where we are today to where we can go in the future and the investment required," he said. Since then, his team has assisted other functional areas within the business to develop their own risk-management plans. "It has nothing to do with cybersecurity other than we're trying to get everybody speaking in the same risk language, such as exposure and mitigation methodologies across the enterprise. This is an example where the CISO is serving as a business leader, which is definitely ideal."

As the meeting drew to a close, Raj asked a final question: What does the future hold for CISOs? What is their next career move?

> "For sure I know that I don't want to be doing this for another 20 years. My hope is that in the next few years, that job that doesn't exist will show up and it will be better than these four options we talked about today."
>
> – **Fernando Blanco**, VP & CISO, CHRISTUS Health

"I think there are three paths," said Jennings "You like what you're doing so you stay where you are; you take the CIO route; or you move to a bigger organization as a CISO." Fernando Blanco, Vice President and CISO of CHRISTUS Health, added one more: risk compliance. But none appeal to him, he said. "For sure I know that I don't want to be doing this for another 20 years. My hope is that in the next few years, that job that doesn't exist will show up and it will be better than these four options we talked about today."

Unpacking the Reporting Structure

Only about a third of organizations have a CISO who reports to the Board of Directors, one survey found. Yet such a reporting structure results in lower financial losses from cybersecurity events. Among the CISO participants, most reported to the CIO.[7]

However, there is no perfect reporting solution, they all have their challenges, asserted Walker, who, during his career, has reported to the CIO, the CFO and the CLO. "With the CIO, if you report incidents that are embarrassing to him, you've got a problem on your hands. The chief legal officer doesn't understand the technology, just the legal impact; and the CFO is primarily worried about spending."

Decker, who reports to the CIO, likes the arrangement because it makes it easier to get support from IT and to integrate IT into the operational side of security.

Bowden, however, made the point that reporting structure is secondary to leadership. "If you can't lead and influence people to learn and do the right thing, it doesn't matter who you report to. If you can lead and influence, you can get the job done."

Wrapping Up

Before concluding, each participant listed the most valuable thing they learned over the past two days. Key takeaways were:

- The value of an internship program;
- The breadth of the CISO role in healthcare;
- The potential of embedding a lawyer within the IS department;
- Identifying opportunities for improvement to continue driving the organization forward;
- The need to push vendors to make changes from an industry perspective;
- Thinking more about next steps in terms of career and long-term planning;
- Regular architecture review meetings.

Endnotes

[1] Deloitte Consulting. Overcoming the threats and uncertainty Third-party governance and risk management (TPGRM) global survey 2017. Available at: https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/risk/deloitte-uk-third-party-gov-risk-management-2017.pdf

[2] Farahani B, Firouzi F, Chang V, et al. Towards fog-driven IoT eHealth: Promises and challenges of IoT in medicine and healthcare. Future Generation Computer Systems 78 (2018) 659–676.

[3] Ponemon Institute. Medical Device Security: An Industry Under Attack and Unprepared to Defend. May 2017. Available at: https://www.synopsys.com/content/dam/synopsys/sig-assets/reports/medical-device-security-ponemon-synopsys.pdf

[4] PwC. Strengthening digital society against cyber shocks: Key findings from The Global State of Information Security® Survey 2018. Available at: https://www.pwc.com/us/en/cybersecurity/assets/pwc-2018-gsiss-strengthening-digital-society-against-cyber-shocks.pdf.

[5] https://cybersecurityventures.com/cybersecurity-unemployment-rate/

[6] (ISC)². Hiring and Retaining Top Cybersecurity Talent. Available at: https://www.isc2.org/isc2-hiring-and-retaining-top-cybersecurity-talent

[7] https://www.csoonline.com/article/3278020/leadership-management/does-it-matter-who-the-ciso-reports-to.html

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 strive to achieve clinical integration and transformation through information technology (IT). SI facilitates knowledge sharing by providing intimate and informal forums that embrace SI's "Three Pillars:"

> Collaboration
> Education
> Networking.

SI Affinity Groups offer a popular way to focus on a shared issue, topic or collective challenges. They can be title-specific or a mix of executive titles focused on single issues like Digital and Population Health, Cybersecurity, Clinical Decision Support, Data and Analytics and others. Affinity Groups convene in a variety of ways including Dialogues, Summits, Ad Hoc Queries, Site Visits and Roundtables.

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.