From Foundation to Future

SCOTTSDALE INSTITUTE 2022 CISO VIRTUAL SUMMIT

May 11, 2022 | Virtual Event

Sponsored by:

Deloitte.
Executive Summary

So much of healthcare IT—from security to digital to confidentiality to integrity—requires technical advancements, interoperability and the strategic genius of those who know the pros and cons of what they’ve built from the ground up. Every addition—of users, programs, governance requirements and organizational protocols—can buoy or sink a system so delicately balanced...and it seems these days, to keep moving forward, we’re constantly adding instead of subtracting.

Desiring to equip and empower CISOs to do that well, the Scottsdale Institute (SI) convened 23 information security officers and special guests to share and learn from each other what’s required to build for the future on the strongest of foundations. Topics included:

- **Balancing Human Resources**: Using Business Chemistry insights to better understand individuals’ personalities and drive stronger, healthier relationships and outcomes with staff, peers and stakeholders;

- **Tackling Digital Consumer/Product Strategy**: Studying the impact on cyber security program considerations as organizations look toward engaging customers and leveraging data and “products” as part of their business models; and

- **Cultivating Cyber Hygiene**: Discussing the challenges of and approaches to managing cyber hygiene, and balancing the elements [e.g., asset management, patching, infrastructure, business continuity, 405(d)] that also impact cyber risk at the enterprise level.
SUMMIT PARTICIPANTS

David Anderson, MS, MBA, Director, IS Operations, AdventHealth
Jeff Bontzas, CISSP, CHISL, VP of Information Security & CISO, Ascension
Michael Czumak III, VP & CISO, Memorial Sloan Kettering, Cancer Center
Rajesh David, CISO, Rush University Medical Center
Erik Decker, CISO, Intermountain Healthcare
Michael Erickson, CISO, Baptist Health
Sam Githinji, CISSP, CISM, CRISC, MBA, CISO, Children's Minnesota
Matt Heign, MBA, VP & CTO & Interim CISO, UW Health
Tricia Julian, CIO, Baptist Health
Jigar Kadakia, MBA, Chief Information Security & Privacy Officer, Mass General Brigham
Thien Lam, VP & CISO, BayCare Health System
Larry Lidz, CISO, CX Cloud Business, Cisco
Janice Maragakis (not pictured), Change and Communications, CPX Security, Cisco
Ron Mehring, VP Technology and Security & CISO, Texas Health Resources
Wendy Perchick, SVP, Strategic Planning and Innovation, Memorial Sloan Kettering Cancer Center
Robert Perry, CISO, Carilion Clinic
Peter Rucys, CISO, Tampa General Hospital
Shenny Sheth, DEE, ITIL, PMP, CISSP, CCSFP, CICISO, Deputy CISO, Centura Health
Pavel Slavin, VP & CISO, Froedtert & Medical College of Wisconsin
Ryan Smith, MBA, COO, Graphite Health
Teresa Tonthat, VP, IT & CISO, Texas Children's Hospital
Patrick Voon, CISO, Loma Linda University Health
Vugar Zeynalov, CISO, Cleveland Clinic

CONVENER
Scottsdale Institute
Janet Guptill, FACHE; Cynthia Schroers; John Hendricks; Karen Sjoblom; Stuart Hurley, FACHE; Margaret Shea; Courtney Olson; Genevieve Hedland-Hill

SPONSOR
Deloitte
Moderators:
Raj Mehta, CPA, CISSP, Partner; Julie Bernard, MBA, Principal

Writer: Karen Sjoblom
Introduction

So much of healthcare IT—from security to digital to confidentiality to integrity—requires technical advancements, interoperability and the strategic genius of those who know the pros and cons of what they’ve built from the ground up. Every addition—of users, programs, governance requirements and organizational protocols—can buoy or sink a system so delicately balanced… and it seems these days, to keep moving forward, we’re constantly adding instead of subtracting.

Desiring to equip and empower CISOs to do that well, the Scottsdale Institute (SI) convened 23 information security officers and special guests to share and learn from each other what’s required to build for the future on the strongest of foundations. But perhaps the most critical element to laying the groundwork for success involves Business Chemistry—that is, studying the relationships and personality mixes that can help (or hinder) their efforts.

Balancing Human Resources

Deloitte moderators Raj Mehta, CPA, CISSP, Partner, and Julie Bernard, MBA, Principal (right), kicked off the summit by acknowledging that dealing with people can get very messy very quickly. “How can I drive influence vertically and horizontally, knowing that people respond very differently?” Mehta asked. “Business Chemistry is a great tool, because it’s focused on interaction, not introspection, and it’s rooted in science while being designed for business.”

“Ther’s nothing more important than managing stakeholders during times of stress,” added Bernard. “Business Chemistry is different than other tools like the Myers-Briggs Type Indicator® because it helps people figure out what their audience needs as well as how they’re going to decipher and react to the messages they’re receiving. Our focus today is to help us understand ourselves and others, and use that knowledge to adapt our styles.”

Deloitte’s pre-Summit survey revealed that 50 percent of respondents considered themselves Drivers, while the remainder were split, 25 percent each, across the Pioneer and Integrator categories (see following graphic). Interestingly, no one considered themselves a Guardian.

“If, collectively, these respondents were a team, I’d caution them about blind sides,” Mehta said. “They’d not be fully aligned before going off on a specific direction…and that’s what Business Chemistry aims to prevent.”
Bernard then discussed shared traits within this matrix and subsequent amalgamated behaviors (graphic, below); for example, Driver-Guardians can be more disciplined, contain their emotions and question ideas. “If you trust someone, you’ll trust what they have to tell you and you’ll trust their data. But if you’re a questioner of people and ideas, you’re going to fixate. That can be a hard work-around when you’re dealing with both trusters and questioners on the same issue,” Bernard explained.
She then provided examples common to traditional work interactions:

- **Pioneers** might change their virtual backgrounds multiple times during a Zoom, or rush to fill the silence
- **Guardians** are most likely to have their video stream off during a Zoom call
- **Drivers** will leave meetings on time—regardless of whether the meeting is done
- **Integrators** will be excited to see someone's pet or child on camera, or might schedule a call just to check in

“People might expect CISOs to have Guardian traits, but we shouldn’t make assumptions whether someone can or cannot do a certain job because ‘they’re just not that way,’” cautioned Bernard. “I have a great story about a Pioneer in a Guardian-type role who added automation, got the team to do things they didn’t think they could, and ultimately got their size and cost down so they could go tackle something else. It’s important to not put people in boxes because of their Business Chemistry or their business card.”

### Tackling Digital Consumer/ Product Strategy

“Raj did this Business Chemistry exercise for our cyber organization and it was really interesting to discuss where we thought we were. It seems like cyber people all are Drivers…but what are we missing? How can we round out our teams?” asked Erik Decker, AVP & CISO, Intermountain Healthcare. “We want to focus collaboratively on the change we believe is happening in healthcare—what digital means, and what platforms and products are involved. We’re going through both evolutions and revolutions on that front and, as CISOs, we’re dominant in thinking about all things and protecting the enterprise as a whole.”

Moderating a panel to consider the different facets of digital consumer/product strategy, Decker introduced speakers Wendy Perchick, SVP, Strategic Planning and Innovation, Memorial Sloan Kettering Cancer Center; Ryan Smith, COO, Graphite Health; and Larry Lidz, CISO, CX Cloud Business, Cisco.

“As a frame of reference, I don’t think about product security as something we buy and implement, but rather that we establish and build products, often digital, and we have a market that demands more access/connection into our healthcare systems,” Decker outlined. “In some ways, market pressures might force function...so how do we build safer products?”

**WENDY PERCHICK: STRATEGY & THE FUTURE**

“I’ve been at MSK for 45 years; MSK itself has been there almost 140 years. Our organization has made many transformational journeys but all have one overlying theme: What we’re seeing always is a mashup between evolution and revolution. There are elements of what existed before—they persist—but what emerges out of it is like new life-forms, and that’s where the opportunity and challenges lie.

“For our framework on strategy, we look at where things are different than before. First, consumers want...
convenience and to be able to access healthcare while in their living rooms in their PJs. But it’s more than just convenience: It’s connection, simplicity and sufficiency. Our consumers are not looking to be overwhelmed with too many options in the market, but that’s almost the definition of American Healthcare. Our second lens considers traditional industry players (e.g., providers, insurers, etc.); their behaviors are changing as well. And third, we look at new entrants—those starting to create new digitally enabled systems—even though we don’t know yet what those will look like, or who will win or lose.

“MSK started in 1884 as the first cancer hospital in the US, and the second in the world—the best scientific knowledge at the time encompassed in brick and mortar. People were inpatients in that model, and we owned everything. But as we progressed toward 2000, technology started to change some things. We gained the ability to look inside of a patient, to diagnose earlier and intercept disease without doing major surgery. It was essentially the same model otherwise, but we moved to an outpatient care delivery system, which broke the link of being able to see all our patients in one space and have stronger feedback loops.

“Post-2000, technology and innovation were accelerating at such a rate that it was changing the nature of scientific discovery and thus our expectations. We saw the potential of scale of being able to interact 24/7 in a highly fragmented way. New entrants were able to match supply and demand; suddenly, on the periphery, we had more options for access. I’d argue now that what we’re seeing—and I’m excited about it—is how they all come together.

“We’re moving closer to center, expanding to more holistic platforms, collaborating and integrating with healthcare providers, and using technology to do something different—moving expertise from 1:1 moments between doctors and patients to 1:Many. We’re improving skillful delivery through feedback loops and observations. But healthcare organizations change very slowly; new entrants, driven by new business models, will force change in the industry. It’s those forced changes we’ll respond to—to see which organizations are showing adaptive strain and are able to create new structures within. If we don’t do it, the new entrants will…and we’ll find ourselves in a lower position.

“It’s not so much whether we’ll have a product, but rather will we be able to take and reintegrate it at the level of a person who needs this for their treatment? Is MSK trying to build every product? No—we’ll never be able to achieve that. But then, are we just contractors? No: We’re masterful integrators orchestrating delivery of care.”

RYAN SMITH: THE DIFFERENCE OF DIGITAL

“Graphite Health is a software company intent on transforming the digital future of healthcare. Backed by leading health systems, we are catalyzing a collective action effort to improve patient outcomes and lower costs. Graphite’s application platform, software development kit, and marketplace empower health innovators and software engineering teams to accelerate health application development.

“We’re not really a vendor or a healthcare organization; Graphite is a not-for-profit, member-backed organization that is pursuing a Healthcare Utility Model. For our operating principles, we’re anchored in the good of the collective. Nobody owns the company; we’re a
501c4 whose initial governing members include SSM Health, Presbyterian Healthcare Services, Intermountain Healthcare, and Kaiser Permanente with plans to enlist additional governing members in coming months with the goal to digitally transform healthcare together. We believe it’s too difficult to solve alone: Health systems can spend up to two years, on average, to implement new digital tools and then have to fully commit before they can ever make use of them. Graphite Health wants to overcome these challenges through the collective power, scale and knowledge of its members. Creating a common data language, or *lingua franca*, toward plug-and-play interoperability, Graphite Health wants to facilitate digital transformation through its data standardization service and open and trusted application marketplace.

“My definition of digital is *the innovative meshing of new technologies, data intelligence, re-imagined workflows and organizational leadership, all aligned to achieve a “sticky” and optimal experience*. It means inviting end-users to virtually access all relevant information while offering a breadth of interactive, automated, self-service capabilities available any time, day or night, using any preferred device, from any connected location. So: What’s really different between digital and IT? Digital only happens with a lot of IT, and this definition is very different from traditional IT offerings. This is a new realm of creating new services and products (see graphic), and then having partners purchasing and deploying these kinds of products in their organizations, either on-prem or in the cloud.
“For us, trust is the name of the game. We will never treat patients like products, and we put transparency and purpose before profit. In fact, we’ve adopted the Digital Hippocratic Oath that helps patients understand how their health information is (and is not) being used. We believe this will be especially important as new regulations transfer some responsibility for security and privacy of the data to the patient. We’re focused on autonomy (the patient directs how their data are used); beneficence (making healthcare easier to access, understand and use); non-maleficence (protecting and securing patient data and never selling it to third-parties); and justice (asking “What would I want for my own patient care and for my family?”). This oath is Graphite’s moral compass, used to create the standardization requirements that enable the creation of a Certified Digital Apps Marketplace. Part of joining our work requires adopting this commitment to treat patient data with the utmost security and respect.

“A key challenge has been the industry’s inability to meaningfully exchange data and really leverage the data we have. It takes big teams and a lot of painstaking work to deploy new patient-facing apps, and a fundamental issue is our lack of data interoperability standards. To overcome this, we’re building semantic interoperability—to standardize data meaning and thus be able to deploy apps in the Graphite environment. As a collective of aggregated member organizations, we will offer our members standardized purchase agreements, integrated cyber review processes, a common Business Associate Agreement, standardized development tools/software development toolkit, and a full-stack cloud deployable platform that member organizations can adopt as their primary platform to enable digital transformation.

LARRY LIDZ: Q&A AROUND PATIENTS, PRODUCTS AND TRUST

“Cisco is a company that has grown through acquisition. In general, we haven’t done significant amounts of integration for acquired companies so, to the customer, it might feel like they’re dealing with 60 companies to address their singular problem. This has been because we’re optimized for growing the top line versus optimized for protecting the bottom line. The problem, though, is that puts the pain on the customer...particularly when it comes to understanding what they have in terms of Cisco assets and how to use them. Moving into my role and thinking in a product mindset has required coming to terms with this focus on the top line rather than driving efficiency to protect the bottom line.

“The organization I’m in didn’t exist a few years ago; making that shift has been interesting in terms of this integration mindset. It’s more about trust and transparency: If our customers don’t trust our cloud environment or the front door, they won’t trust us. No one will use our products. At Cisco we’re lucky that we have customers who grill us about what we’re doing and how we’re protecting them. It’s an advantage of being a primarily business-to-business company. Those companies providing services directly to individuals may not have this transparency. But the general thought needs to be the same: What is it that our customers are expecting? How can we do right by them? I believe everything will fall into place if we focus on those two things first.
**Erik Decker:** What are some core elements of these trust programs? It’s something new for CISOs to think about.

**LL:** I think it’s much of what you already have in place (e.g., the controls and how they work). But the difference is that you also need to think about how you pull things together—how you package and present to your customers. It’s not as easy as you’d think: It actually gets complicated from a few perspectives. One, on the back end, the way a customer thinks about a product is often not how we deliver it. The customer might say, ‘I want a, b and c.’ But our back end involves a different group than the one managing the front end; it’s a different org that handles the different components of this service, so how do we wrap this all up with a single bow to hand to our customer? Two, often we’re not having such conversations with our customers directly; they might have security questions but end up asking them of the sales people, who don’t have the full understanding the security folks do. So, again, how can we pull material together and structure it so that it’s available to the customer when needed, and to drive that trust and transparency?

**ED:** To the rest of our CISOs here—do you have any thoughts? Have you started to see more of this consumer-driven/patient-driven expectation around the digital interface? Are you thinking about different products?

**Michael Czumak:** How can we look at security as a feature? Take, for example, multi-factor authentication (MFA). What if we didn’t think of it as an internal mandate, but rather a consumer expectancy to keep their data safe? Should we offer it as a feature? Beyond that, consumers might not expect certain things, but we might offer specific options. It’s just a shift in our thinking: We have to look differently at how and what we’re building around our consumers and their expectations. There’s a big difference between viewing security as a value-add versus a requirement.

**LL:** Cisco is a product management-driven organization, and what became apparent pretty quickly is that most thoughts around security entailed reducing friction—as in, ‘Nobody wants MFA—that introduces friction.’ But no one will deal with us if we don’t offer it! In fact, consumers may look for different providers if MFA isn’t offered. Our trust requirements trump our product requirements. We incorporate MFA to maintain our customers’ trust. We may have to swim upstream with that here, but my responsibility is to be a representative of our customer security teams when they’re in the rooms. Product managers don’t necessarily understand this trust mindset.

**Jeff Bontsas:** I agree 100 percent with Larry. Customers are getting more accustomed to MFA with their banking accounts and other services. They understand it’s not just an option, but rather a necessity to have that security around their records. In our organization, one of our main strategies now is around the consumer experience. We know more and more that the experience people have around Amazon, for example—when they can move quickly and navigate easily—is the direction healthcare eventually needs to go. We need to offer that kind of service but it’s even more challenging for us, with a legacy environment, to move that way in the future.
**Ron Mehring:** A couple of years ago, we changed how we handled enterprise-level cyber risk and created a consumer-digital risk domain. At the time, our program was not focused on the nuances of consumer delivery (e.g., MFA, self-selected passwords, preference management, scheduling). We inventoried our consumer systems and related data and associated it with a consumer-digital risk domain. We then dedicated security staffing toward the secure delivery of consumer-digital services. We recognized that agile delivery is unique and very different from traditional IT. We also learned that agile delivery should not be conflated with conventional IT service delivery and that dedicated security processes for this risk domain would be an effective way to support consumer-digital delivery objectives.

On the consumer trust side, at the healthcare delivery level, we have a preexisting trust, an implied covenant with our patients. People who interact with a healthcare delivery system already have a built-in assumption that their data will be protected.

**ED:** So what happens if that trust is broken? Would they choose different providers?

**RM:** A small percentage might walk away, but I believe most would stay. People are there for different reasons. They might walk away from an app, but not from the delivery.

**JB:** I care about data breaches, but we absolutely must think about patient safety. If anything is being compromised, if dosages are not accurate... There needs to be a huge focus on cyber security and not just data.

**RM:** When we design for safety, it doesn’t go through the consumer arena. We don’t comingle the consumer arena with patient safety.

**Pavel Slavin:** Before the pandemic, a subsidiary company of ours invested heavily in consumerism, which resulted in some go-to-market products. That opened up some interesting propositions: How do we deal with consumers versus our IT security? Our approach is similar to Ron’s. We mostly remain present and offer direction. We’re still accountable for the security of a solution. If there’s a problem, the CISO is responsible and accountable, so we’re trying to make sure we have policies that are applicable to consumer-oriented products.

**LL:** I think the bottom line is that everything must be agile. Things change really fast in our industry. In my perspective, one of the most important things for us, as leaders, is to not assume that we don’t need to worry about risks just because they’re unlikely to happen to us. You might have great controls to protect patient safety, but it only takes one organization that doesn’t before the industry changes... and then the questions you’ve been asked by customers to maintain their trust change overnight. We must be willing to adapt and change quickly.

---

**Cultivating Cyber Hygiene**

**CREATING A MORE SECURE MEMORIAL SLOAN KETTERING**

“When you think about the foundations of cyber hygiene, every industry struggles with how to manage risk when you’re dependent on other parts of the organization,” said **Michael Czumak III**, VP & CISO, Memorial Sloan Kettering Cancer Center. “At MSK, we have multiple aspects of what we do (multi-state locations, a grad school, multiple facilities, plus a research institute with 160 labs) that push us regarding our digital strategy. I was the first CISO at MSK, and I’ve been here eight years. At first, we needed the basics; now, we’re maturing beyond those basics and introducing new capabilities. But we’re also shifting the conversation from a security only program to how we’re holistically managing cyber risk. It’s far more than just what’s happening in our program.”
relationships involved in the technology lifecycle? They’re all fundamental to cyber risk, but I’m not managing all of that. It falls outside of my construct.”

Czumak suggests lumping the remainder under the umbrella of “cyber hygiene.” Defining that as a set of ongoing lifecycle management activities (technology, data, vendor) that’s necessary to ensure an environment remains healthy and resilient to adverse events that could interrupt or threaten operations, confidentiality, data integrity or availability of systems, Czumak explained that MSK has a funded program specifically for hygiene. While multiple parts of the organization may be responsible for different facets, all are tracked centrally, with assigned accountability and reporting as part of MSK’s cyber risk management approach.

“How do we get our arms around cyber hygiene collectively? Executive owners had been established with their own verticals but, ultimately, who would be responsible for the day-to-day technologies that we all rely upon?” he questioned. “We needed to establish a role for that, as well as develop a community of tech owners across the organization and help them carry out these hygiene responsibilities.”

Defining cyber risk management as the set of all technology- and security-related activities required to ensure the confidentiality, integrity and availability of critical data and systems, Czumak believes “cyber risk” encompasses everything organizations need to consider to protect against events that could cause disruptions. “If we were to map out our security program coverage to the NIST Cybersecurity Framework (identify, protect, detect, respond and recover), then we’re only doing about 60 percent of what’s suggested to safeguard against all cyber risk. What about the other 40 percent—the patches, upgrades, data backups, testing procedures and vendor...
MSK’s practical approach uses a pyramid visual that depicts the various layers needed for success (see graphic).

Czumak explained how these layers have worked well for MSK:

- **Assigning ownership and accountability**: “If no one knows who’s responsible, then no one is responsible. We needed to establish a role for the person responsible for day-to-day technologies that everyone relies upon while also developing a community of tech owners across the org and teaching them to perform hygiene for MSK.”

- **Educating and engaging**: “We’re developing resources and training for folks to understand how to perform our cyber hygiene protocol properly.”

- **Standardizing practices and centralizing enforcement**: “We also want to train people to do things consistently, provide necessary resources, and standardize and enforce our guidelines. For example, with regard to patching, we know we need to keep assets off the network or otherwise segregate traffic if they’re not patched.”

- **Monitoring continuously**: “We delineate responsibility, then operationalize that and ensure visibility. We’re designing dashboards for the different views our stakeholders need, and to also filter out what they don’t need to see.”

“Asset management seems to be top-of-mind for many of us here, and it’s one of the top three focuses for our hygiene program,” Czumak explained. “Overall, it’s helped our teams tremendously to talk about all of it—cyber security, management and hygiene—in one conversation and begin to track it in one standardized way.”

**TERESA TONTHAT: Q&A AROUND PROTECTING AVAILABILITY & MANAGING ASSETS**

“As VP of IT and CISO at Texas Children’s Hospital in Houston, I realized there had to be a shift in the types of conversations I was having. How can we work together to maintain availability of systems?” she wondered. “Our cyber security practices afford us the ability to keep our systems up and running against ransomware, breaches, etc., but if someone has failed to patch or follow standards for architectural design, that goes back on poor hygiene. And honestly, it took some time to get us all on the same bus… but ultimately cyber is everyone’s responsibility.”
According to Tonthat, cyber security is viewed as a strategic initiative today at Texas Children’s; there’s a lot of support from the top down about the need to invest in people and processes to protect operations. But she admits the term “go dark” is fairly new to the executive team; they hadn’t realized the fullness of that—that there would be no access to the internet and that hospital phones wouldn’t work. So while it’s important to get investments and funding for cyber programs, she also believes people need to understand the why behind it—to ask, “What’s in it for me? For the doctors and nurses on the floors?” That’s why it’s important to have conversations at the board level, so it’s more of a business decision, less of a technical one.

“Over the past year, we have intentionally built out our Organizational Resilience team that reports to our supply chain leader, because we feel we haven’t paid enough attention to ‘going dark’ downtime procedures and we needed to refresh our business-continuity plans. For example, when was the last time we did a simulation?” she queried. “If Epic went down, people would know what to do, but if we lost SharePoint, email, PACS systems, etc., we’d lose more access to data than we’d expect. These questions and tests translate into the ability for us to be resilient; the money we spend on refreshing technology and going digital all ties back to our ability to keep going for our patients and members.”

Tonthat has opened a board meeting by sharing about the areas in which Texas Children’s is not quite as strong as it needs to be. She believes any drift around security hygiene, MFA, privileged access accounts, etc., can all contribute to security events.

“One of my biggest concerns is asset management. There’s no central system for all assets. They’re in disparate locations. My fear is, what might I not know about?” she wondered. “What about assets that were purchased blindly without going through our standard process, like getting a free computer from a vendor and plugging it into our system? It’s a people-and-process issue as much as a tech issue.”

Michael Erickson: Asset management is definitely a challenge. We’re looking at procurement from a total lifecycle-management perspective (how things come in and out of the organization) while also focusing on detection and containment of unauthorized or rogue devices. To do this, we are using an innovative new technology that provides layer-1 visibility and hardware access controls to enhance our visibility and control of digital assets, including human interface devices and other peripherals.

TT: Is there a process for bringing software or hardware onto your network without going through your supply chain process?

ME: This is increasingly rare, but if it happens, we have conversations with leaders to educate them about the risks and our procurement policies. The technology I mentioned previously is specifically designed to protect against the risks associated with unauthorized or rogue devices. Through this partnership, we have learned to recognize the importance of monitoring the existence of devices within an environment, not just their activity.

Tricia Julian: I’m the CIO for Baptist and participate on a Discretionary Spend Committee alongside our CFO and COO to review any requests that will create a new op-or cap-ex cost; for us, it’s got to go through committee for approval, including software purchases. If Marketing wants a new cloud partner, for example, we centralize the spending request so that the CIO, CFO and COO all see
it together. The approval process ensures business plans include all associated costs by identifying any required IT resources and confirming IT security questionnaires have been distributed. Spending decisions were more siloed in the past, so the new process improves transparency and collaboration by having more perspectives at the table to approve and deploy funded projects with both agility and excellence. In my five years as CIO, I’m seeing favorable impacts from this multidisciplinary look at solving business problems, and having the right perspectives at the table helps us tremendously in avoiding re-work and surprise costs.

**TT**: But there’s the challenge of going backward to see which equipment is still being used without having gone through the right process. For example, I might be aware of a hundred apps, but then I’ll see media news of ransomware and wonder, “Do we have that product?”

**Vugar Zeynalov**: We are having fact-based conversations to address cultural challenges and change behaviors on how people connect devices to the network. Cyber hygiene is a sort of “population health” problem: How can we declare our digital assets as healthy? We look at workstations, servers and other devices to ensure protection profiles are in place and that the devices are managed, patched, logged in our system, and have appropriate controls.

We brought everything into a central place for viewing so we could tell whether our assets had all their protections in place, but this also helped us protect against “outside” equipment as well. This drove some behavioral change and significant improvement in those areas. Currently, we’re looking at the concept of self-healing, of using the hygiene assets/products we have to close the gaps and trying to better automate our processes.

**Jeff Bontsas**: We are using security tools to help shore up our asset management. We currently have feeds into ServiceNow™ and are trying to make our asset management system more accurate by using Medigate for medical devices and shoring up medical- and Internet of Things (IoT) management as well.

**Patrick Voon**: It’s been a real journey for us. We still have a lot of folks who don’t fully understand our governance process and therefore install stuff on their own. As an academic medical center, we have a lot of openness on the academic side, while the clinical side is more stringent for obvious reasons. Regardless, across the entire organization a lot of business units choose to do things on their own. Unfortunately, we can be viewed as a bottleneck, with all our procedures and standards...and not just for security, but for compliance, too.

**Rob Perry**: We utilized a tool to help us track down the assets that had fallen out of compliance and to get a better understanding of how our machines were being used, especially as workers moved out of our health system to work remotely. We’ve also tried network access control tools but found some too unwieldy. Occasionally staff outside of IT try to buy off-the-shelf or cloud-based software which bypasses our risk management screening process, so we’re trying to rein that in. Currently, we’re looking at IT Service Management tools like ServiceNow to create a centralized database that our ancillary tools can plug into, but we must first develop strong policies and procedures to get everyone to buy into tracking and lifecycle management across all environments.

**Shenny Sheth**: At Centura, we have similar asset inventory woes as others. We aren’t just writing policies, procedures and standards, but rather developing well-architected and -integrated clinical, access management and security solutions to create a cyber resilient organization, with special focus on cyber posture management. We’re remaining transparent to the stakeholders, noting the impact yet managing end-user experiences and marching forward. While early in the phases of maturity, Centura is on a path to becoming a flagship health system—with Cyber and Clinical programs resourced toward envisioning and enabling Hospitals of the Future.

**Ron Mehring**: Cyber hygiene is a complicated realm. When applying cyber hygiene practices and principles to a complex healthcare organization, there are many pieces and parts that must be considered when you look at the whole integrated ecosystem. This ecosystem comprises different, interrelated components and considerations.
such as legal and entity structures, identity types, and technology diversity. In many ways, cyber security comes down to lead time. For example, if you have a vulnerability within the environment that’s known and detected, how long will it take to fix it? How do you design for remediation latency and carried exposure? Our traditional approach to the design and execution of security services has been relatively linear; of course, many of the cyber challenges we face today are nonlinear. Not recognizing the complex, tightly integrated, nonlinear nature of our ecosystem creates significant challenges for cyber hygiene implementation. If we are not careful, we can create downstream compatibility/reliability issues and even more complexity. At Texas Health, we realized this is a technology and security unification problem, a speed problem. We would have to build and organize around these issues differently than we did in the past.

Conclusion

As these healthcare security professionals continue adjusting their foundations and designing their futures, the quality of their raw materials—both human and technological—becomes critical. By building cohesive teams with varied visions who are able to see different perspectives and note potential pitfalls, these CISOs will be well-equipped to elevate cyber security, hygiene and management to meet the health system changes to come.