As cyber attacks proliferate and gain in sophistication across our increasingly connected globe, it is becoming ever clearer that CISOs are the unsung heroes, protecting sensitive governmental, corporate and organizational information from falling into the hands of malicious actors.

The role of Chief Information Security Officer will vary from organization to organization, and no set of skills is the same. But wherever CISOs may be, they must demonstrate an array of proficiencies that include technical knowledge, negotiating prowess, coolness under fire and an ability to anticipate the future. Increasingly, the requirements demanded of a CISO have reached the C-level tier. You are no longer technologists operating unseen in some back room, your skills an afterthought. You have become business leaders charged with understanding how an organization runs and how to balance risks and threats in the interest of its goals.

Growing recognition of the crucial need for cybersecurity expertise is abundantly evident, from the proposals of the U.S. Securities and Exchange Commission, to the No. 1 ranking of cyber incidents and business interruption on this year’s Allianz Risk Barometer, an annual survey of key business risks around the world.

The criticality of your role is of course no surprise to us at CISOs Connect. We know you and your teams are in the trenches every minute of every day. With this inaugural CISOs Spotlight Edition of CISOs Connect Magazine, we’d like to pay tribute to your extraordinary efforts by highlighting the people behind the role -- what drives them, how they approach their job, their visions of the future, and how they cope with the relentless pressures that come with being a CISO.

As a community that gives and learns from each other, you will find much inspiration to take from your colleagues and their stories. Enjoy the read!

Aimee Rhodes
In This Issue

On the cover: Matt Lemon and his son. Read more on page 35. Photo provided by Matt Lemon.
As cyber attacks multiply in number and variety, a lot of CISOs are heavily focused on the technology that defends their organizations against bad actors.

But for Ceridian CISO Colin Anderson, it’s the soft skills, rather than technical expertise, that help him to excel at his job.

“I’m not a tech guy by training,” said Anderson, who studied finance in college. “I didn’t go to school for computer engineering or computer science. I’m a people person. I’m a good communicator, a relationship builder. The tech skills I’ve developed on the job,” Anderson explained.

“When I look back at my career, and at some of my peers who are more technically oriented, I think it’s the soft skills that have helped me in my journey as a CISO.”

Connecting cyber to business

His finance degree gave him an understanding of risk, and tools to evaluate situations, Anderson said. It also gave him a business orientation that he says is critical to the CISO’s role. Good CISOs realize that they’re good business leaders, and connecting cyber to Ceridian’s business goals is the biggest challenge he faces, he said.

That means understanding the priorities of other business functions and how cybersecurity can support them. “I want to make sure that security is an enabler, and not just a risk-management cost center,” he said.

Over the years, the CISO’s role has evolved into more of a business leader, with a seat at the table where strategy is formed. That requires a broader understanding of an organization’s business than was once demanded, Anderson said.

“Not every CISO is a well-rounded business leader. Those who can excel beyond their security domain and be viewed as a business leader will have a greater impact on their organization,” said Anderson, who conceptualized CISO Connect’s Top 100 CISOs peer awards, given in recognition of outstanding talent in the industry.
**Speedily changing technology**
This is not to say that technology isn’t a core issue. The speed with which technology changes is one of the hardest things for any technology leader to deal with, he said. “You often find security playing catch-up to technology.”

The other big challenge these days is closing the talent gap, he adds. To help narrow the speed gap and the talent gap, he’s trying to leverage automation. “I like tools that help me take mundane tasks off humans and have my team focus on the more higher-value and people-centric work.”

**Circuitous path**
Anderson followed an indirect path to the CISO’s seat. Equipped with his degree in finance, he landed a job as finance manager on Bank of America’s trading floor, but he figured out early on that the “cutthroat” work environment was not for him.

“I’m seeing the managing directors in the corner office on their second or third marriages, and second or third heart attack,” he said. “It just was not the career I envisioned for myself. So I started getting into the market data feeds that were supporting the trading floors, and then I got into the security around the trading floors.”

His disillusionment came at an opportune time – the 1990s, when security was starting to take off as different risks began emerging.

“This was really interesting to me,” he said.

**After Bank Of America**, he was in what he called a “dotcom blowup.” He was appointed to his first CISO role at Safeway in 2009, then left after a merger to join Levi Strauss, where he stayed six years before moving to Ceridian.

**Developers of talent**
Throughout, Anderson has put the emphasis on people and process more than on the technology, seeing the CISO’s role as a developer of talent. Mentoring team leaders, building on their individual strengths and investing time with them are priorities.

“Lots of people focus on the new shiny thing and think that will be a game-changer for them,” he said. “I don’t think technology solves broken processes. I look for tech to innovate, and drive efficiency and productivity. But rather than try to mold process and people around the technology, I mold technology around the people and the process.”

Another part of the formula to being a successful CISO involves keeping things simple, he said.

“A lot of CISOs are engineers at heart, and engineers at heart in my experience like to make things too complicated,” he said. “I think CISOs need to invest in relationships and communications. The technology is usually the easy part.”

Execution should be another key focus, he said.

“I think a lot of CISOs like to focus on strategy and the big-picture plan, but you can’t take your eyes off execution. It’s really easy for the wheels to fall off the bus.”
Supply chain worries

Challenges in cybersecurity have shifted, Anderson said.

Many CISOs are becoming more worried about their supply chains as organizations move increasingly into the cloud and become more dependent on partners to allow them to deliver services, he said.

Business resiliency is also becoming a bigger issue as organizations face a constant slew of attacks, he said.

“We’ve always focused on the paramounts of confidentiality and integrity and availability,” he said. “But these days, I think resiliency is even more important because the reality is, we are all under attack.”

Application programming interface is another worry. While API offers businesses a lot of opportunities, there’s a lot of risk that CISOs have to manage at a very swift pace, Anderson said.

Decompression chamber

With all the pressures a CISO faces, Anderson looks to the great outdoors to unwind. He lives in the California hills, and takes advantage of the good weather to mountain bike with his children, and hike with his wife and dog. He also listens to a lot of music and books on tape. “I like to unplug and let my mind wander,” he said.
JAMES BLAIR

TODD ENERGY CISO
James Blair launched his career in cybersecurity on the service desk at an Australian energy company. Starting from the bottom up has definitely shaped how he executes his role as CISO of Todd Energy, a leading natural gas provider based in New Zealand.

"Initially, cybersecurity was very reactive," Blair said. "It's great for that dopamine rush, but you don't normally move forward all the time when that's the approach.

"As a result, I became very strategically focused. I develop a plan and execute from there, adapting the plan when necessary, but without being reactive all the time. You've really got to know where you're heading and how you're going to get there."

In the future, he sees the CISO's role evolving in a more collaborative direction because of the expanding threat landscape.

"Cybersecurity is a global issue, not a local or regional or national one, and people need to collaborate and talk more. So forums like CISOs Connect, which have established global networks of excellence where you can actually reach out and talk to people, is where I see the CISOs gaining exceptional value," he said.

"These sorts of forums allow you to communicate with people at the same level, with people who have the same challenges, to talk about different ways they've done things and then take that information, distill it and formalize that into your plan. I think that's a really good platform to work off of."

Blair was born in South Africa, left to travel around the UK, then moved to Australia and later to New Zealand. In his free time, he rides motorbikes, and goes biking with friends in the hills and backcountry of his adopted home. He also likes to golf and boxercise, a sport that emulates the fitness required for boxing without the full physical contact.

He sees a direct line between the kind of off-duty activities he enjoys and the work that he does. "I'm hell of a competitive," he said. "I've always wanted to get to the top and I like to fight outside my weight division as well."

"Our digital program at Todd Energy has won Asia Pacific and global accolades, and I'm also on some global committees, which is unconventional for a company our size. We do that through merit, showing that even relatively small companies have significant amounts to offer. We have to be very entrepreneurial in our execution, and that probably differentiates us."
Like other CISOs, Blair faces resource challenges that are made more complex by New Zealand’s geographical isolation and population of just over 5 million.

“There is a skilled resource gap globally in this space, but certainly in New Zealand, there’s the added complication of finding skilled resources locally,” he said. “There’s also the challenge of retaining people you’ve trained, because there’s always the risk that the people you’ve trained will leave to go to bigger, better jobs because there are so many opportunities in the space.”

As for financial resources, money is always a challenge, but that encourages creative thinking, he said.

His broader remit includes overall responsibility for the company’s digital transformation.

“I was over the in the U.S. recently at a conference, and it showed that the breadth of generalization is certainly more prevalent in New Zealand than a lot of the U.S. companies we saw,” he said.

**A successful CISO needs to look at things holistically and be able to network effectively, Blair said.**

With resource crunches, Blair expects to see more virtual CISOs coming on board. Another trend he sees is more alignment and/or adoption of standards.

“Governments, especially around country critical infrastructures and privacy, are requiring businesses to comply with defined requirements,” he said.

Blair regards cybersecurity as a long-term game that involves a lot of change management.

“It’s not just about bringing the IT people along for the ride, it’s about bringing the business along for the ride,” he said. “That includes senior executives so you get their buy-in, and even our operations personnel. Everyone in the organization needs to know how to initiate the incident response plan, why they need to update their PC regularly, why they need to do cybersecurity training. Cybersecurity impacts everybody in the organization.”

His program works on a building block model.

“We started with step-change improvement because we didn’t really have the cybersecurity program or team in the beginning,” he said. “But now it’s iterative improvements to maintain and sustain our overarching maturity. Cybersecurity is continuously evolving, and you need to continuously allocate resources.”
“It’s not just, follow the next trend. You have to be able to analyze things effectively, and have the ability to communicate and problem-solve rapidly,” Blair said. “Communication is key. It is our role to make it easy for boards and executives to understand what they need to do to make the organization more secure, and that requires you to be a very effective communicator.

“You also need to be adaptable,” he said. “If you’re going down a path and it’s not working, you need to be able to acknowledge that and change tack.”

His advice for people just entering the field: Get as much experience as you can.

“Get a wider view of things instead of just looking at a security tooling,” he said. “Not just in the networking realm, though obviously networking is a key place to get experience. If you get a depth of experience in multiple IT areas you’ll definitely be more effective.”

Blair prides his team on developing a culture of cyber awareness at Todd Energy that spills over into people’s home life.

“The biggest thing is that we’ve brought the organization along with us,” he said. “We’ve made them more cyber aware and as a result cyber safe, and then they take that cyber awareness and cyber safety home and share it with their families, and it becomes part of how they interact digitally.

“They end up mitigating risk for you by not going into unsecured networks in the airport, or using short passwords that get compromised. They also take those cyber resilience skills into other organizations. They become good digital citizens. It’s really cool.”
SUZY CLARKE
XERO EXECUTIVE GENERAL MANAGER FOR SECURITY
After living nearly 20 years in New Zealand, it’s a concept native to her adopted country that guides UK-born Suzy Clarke in her leadership role.

“Kaitiakitanga, or guardianship, is a concept that comes from the indigenous people of New Zealand/Aotearoa, the Maori, who talk about being a good ancestor,” said Clarke, executive general manager for security at Xero, a global developer of online accounting software.

“That cultural influence has shaped my thinking about taking the long term view of leaving the security industry better than I found it, and contributing to improving things like gender diversity where I can. One of the things that we’ve been doing recently is asking, are you a good ancestor? Not, are you making the most of what you’ve been given, but are you actually paying it forward?”

Clarke has been working in technology for 24 years, beginning at an IT startup in England. It was there, looking at the company’s firewall logs, that she became fascinated by the fact that this tiny company in England was being targeted.

“Now, I know people were just sort of sweeping the internet. But it really sparked my interest in security, and so it became an area that I specialized in,” she recalled.

She got her start in banks and consultancies, and within a few years had moved to New Zealand where, as a pen tester at a bank, she discovered a very creative side of things in addition to the technical work.

“It was there that I saw the power of a very high-performing team,” she said. “There’s something very special about that moment because it really showed me not only how you could have a really fulfilling, engaged and engaging job, but also how you could build an amazing team by picking the right people.”

With that realization, Clarke understood that she wanted to be in a position to create things.

“I decided that people management and people leadership was more a calling that I wanted to try, and the bank supported me to do that and put me on a training course.”

For the past 14 years, she’s been leading teams in a variety of roles. Her career has included positions at ASB Bank, sustainable clothing maker Icebreaker and Cap Gemini Ernst & Young.

When the opportunity at Xero came up, it brought together three things for Clarke: the security background, the leadership, and a desire to contribute in New Zealand, which allowed her to move there to help plug a cybersecurity skills shortage.

“It offered the opportunity to work for a Kiwi company that was trying to go global and make a positive impact on the world from New Zealand,” she said. “I was absolutely drawn to that.”

The evolving threat environment is a major challenge for all CISOs today, and is something Clarke is very focused on combating.

“I’m always thinking about how we stay ahead of the evolving threats,” she said. “We know the temperature is rising out there, and we have the added challenge of managing those threats while we grow and scale from a New Zealand-based business into a truly global player. This means we need to work very fast and ensure we provide multiple layers of protection to our customers.”

Supply chain risk, the use of artificial intelligence and machine learning as attack tools, and the rise of nation-state assaults on private organizations are major trends she identifies. Threats have accelerated, and there’s also the wild card factor, she said.

“You just don’t know what the really next big thing will be,” she said. “We have to be agile and aware and tuned in enough to be switch on to respond when it does appear, because some of the stuff comes out of left field, like the commercialization of ransomware, which has become a business model!”

One of Clarke’s many mentors said something to her that has served as a lodestar: Learn from everyone, be it a barista or a CEO.

“If they’re doing a great job, how is it they’re doing that? What is that amazing thing? And if they’re not doing a good job, then think, that’s not the leader I want to be and learn from that, too.”
It took four or five years before Clarke worked with another female on a security team, and much longer before she reported to a female.

Recently, her team at Xero won the Best Place for Women to Work in Security Award at the inaugural NZ Women in Security Awards. At the time, 33% of Xero’s security team were female, and junior team members were 57% non-male. That’s sharply higher than the industry average of less than 20%, which was the level the team was at when she joined Xero in 2019.

“I know the lived experience of being the only female for years at a time, so I felt the obligation to improve things for the better,” she wrote in a recent article. “Also, as a gay woman, I know the difference between having a diverse team and truly having inclusion.”

Clarke worked closely with Xero’s talent team to identify and approach female security leaders, and tasked colleagues with increasing female diversity within the leadership team. She also broadened the potential talent pool by focusing on candidates who could bring curiosity, culture fit and a hacker mindset to their roles, rather than specific security experience or certifications.

“That included us hiring many new team members from adjacent roles within Xero,” she said.

Xero’s corporate culture encouraged diversity, she said. The company recently installed its first female CEO, and the executive leadership team is more than 40% female.

Another innovation at the company that Clarke takes pride in is the productization of the security function internally.

“It’s us trying to make the engineers’ lives easier and understanding how to enable them more instead of regarding ourselves as separate from everything else that’s going on in this company,” she said. “It’s been incredibly effective.”

Over the years, Clarke has seen the CISO’s role evolve in importance as security increasingly becomes a business concern. She reports to the board, and took a director’s course to understand what directors care about, what language they use, and what perspective they take on a business.

“She literally just sort of stood in their shoes and realized, that’s how they see it,” she said. “And then I was able to align with them more and talk to them in the way they talk to each other.”

Aside from business acumen, today’s successful CISO needs a growth mindset and “deep, deep resilience,” she said, laughing.
With such a high-pressure job, Clarke loves being active and off-screen.

“I love surfing, playing soccer, things where I have to be really present and can’t be fiddling with my phone,” she said. “When you’re out on the water surfing, it’s a multiple hazard environment. You’ve got to be aware of other surfers and the waves and sharks, so it puts you in this really present state. It also gives a sense of connectedness as well, that sense of flow that you get.”

To young security professionals, she advises “stay curious, and find a way to hold on to that beginner’s mindset.”

“Don’t be afraid to ask questions, because sometimes that is the thing that unlocks the solution that other people who are perhaps a bit more expert or experienced are overlooking,” she said.

She also recommends against specializing too early.

“Rotate yourself through a lot of different areas and find the one that lights you up, because there are going to be some hard days in security, and you want to have that high engagement that puts you on the front foot,” she said.

One of the things that Clarke loves best about the security field is “people’s willingness to support each other.”

“We all do lean in to try and help uplift the industry,” she said. “Sometimes we think we’re sort of competing, but on some of the key things in security we need to work together, so it’s more collaborative.”
Being a CISO “is a lifelong learning adventure,” says Roland Cloutier

He should know. His professional trajectory has taken him from military law enforcement to Global Security Chief at TikTok and soon, a special adviser to the mobile video hosting service.

“Don’t think because you have one certificate that you’re great for the rest of your life,” Cloutier said. “Make it your passion to learn about your trade, your craft, your business. Whether you’re 21 or 51, you need to be a continuous learner in what we do every day.”

Bitten by the cyberbug

It was that thirst for knowledge that got Cloutier into the CISO business to begin with. While working in law enforcement for the military, he discovered that many of the cases dealt with technology and computers. At first, he’d confer with friends who’d help him, but at one point they suggested he go back to school to learn the material firsthand.

“I just got bitten by the technology and cyberbug,” he recalls. “I loved it.”Within a week of graduation, he had a job, and soon discovered that there was a void in developing crucial infrastructure programs for corporations. He built programs for EDS, then went out on his own with a company he later sold to Global Network Technology Services (GNTS).

After he helped three other companies build their capabilities, the CIO of EMC invited him to be the company’s first CSO. From there, he went to ADP to build its global programs, and most recently, he was asked to build TikTok’s Global Trust Initiative.

“My specialty is converged security, how do you look at all the aggregated areas of security and put that under an umbrella organization that can represent the risk that the business has and solving those risks without having four or five different people going to the CEO saying the same thing,” he said. “How do you get accountability for the totality of security risk and privacy programs in one organization?”
Understanding the context
Starting out in the military gave Cloutier an excellent foundation for understanding the concepts of what needs to be protected.

“The government spent a lot of money training me on all aspects of security,” he said. “Those concepts of understanding the constructs of what you’re trying to protect, the criticality of it, the risks associated with those things. And then, how do you put programs in place?”

“If you can operationalize that method, you can teach others to do it. You can develop very powerful programs that protect companies and organizations,” he added. “That base training that you get is so important.”

Leadership is key
The second thing the military instilled in him was the concept of leadership.

In the military, “you lead from up front, you find and create great leaders, and you enable them to go execute their mission space,” he said. “Being mentored by amazing people throughout my government and non-government career, and having to understand how leaders should really work when it’s a serious, life-saving program or mission space you’re operating in, being able to take that and teach that, I think, is the other thing that has made me successful.”

Major challenges facing CISOs today
Cloutier identifies three key challenges facing CISOs today.

No. 1 is filling the gap between security expert and business by developing business acumen, Cloutier said. “This is a business job, so security risk and privacy operations practitioners and executives need to understand what they’re protecting. How can you protect the business if you don’t know what they make, sell, deliver, how they profit from it?”

Continuing technical acumen is Challenge No. 2. If a company operates predominantly in the cloud, then a CISO had better know something about cloud security and containers and technology movement between cloud providers, he said. Capabilities have to change as technologies and enterprise operations do: “You should always be increasing your knowledge.”

Understanding what’s happening in your environment is key as systems get smarter, with a lot of them self-defending. That means teams are going to be migrating from technical positions to analysts’ positions. “It’s a whole new job family. How do we train them, select them? That has to happen, sooner rather than later.”

Challenge No. 3 circles back to the leadership discussion.

“You have to adapt as a leader to the changing type of people coming into this organization,” Cloutier said. “The average age in my last company was half of my age. They don’t think like I do, consume information like I do. You have to engage people where they’re at, where they think.”
Trends in cybersecurity

Organizations are moving their programs out to cloud providers, which is a positive development because there are innovations in cloud capabilities that didn’t exist before, he said. That requires CISOs to take responsibility to take advantage of the cloud. “Cloud migration will be a continuing learning experience and issue for enterprises as they do that.”

Another important trend are the golden nuggets that technology companies are pulling from massive amounts of data, Cloutier added.

“Being able to show and prove how we use data is going to be one of the most leapfrogging events in cyber defense operations in the next five years because of the continuing developments around machine learning capacities and advancements in artificial intelligence,” he said.

Giving back

Giving back is a major imperative for Cloutier, whether by guiding a young neighbor into a high school mentoring program, or training people on his team, or mentoring people outside his organization. “It’s a lot of little things, but if we each do them, it becomes a massive effort.”

“If you accept mentorship, and you accept feedback, and you can take that and convert it into how you act and move your experience forward, you’re going to be very successful.”

New horizon

Cloutier recently announced that he would be transitioning from his role as global chief security officer at TikTok into a strategic advisory role, focusing on consumer security initiatives and how they impact the business.

Stepping back and not doing operations any more is going to require re-education, he said. “You can’t just turn it off … You’re wired to solve problems. … That’s how you are.” In his new job, “it’s a different focus,” he said. “Getting back to that part of why security is important for business.”

Kicking back

People have to make the time to detach themselves from work, Cloutier said. He’s an outdoors type, and likes to spend time on his daughter’s farm, where she runs an equine program. He also enjoys fishing and semi-competitive shooting, and recently started hiking, most recently in the White Mountains of New Hampshire. Reading books that aren’t work-related — Tom Clancy is a favorite -- is another outlet.

“People have to find the thing that disconnects them so they’re not thinking about work, they’re not looking at their iPhone or their devices, that they can totally get into, and get out of their head space and give themselves a little bit of rest.”
Working with a mentor who understood that security must be viewed within a broader lens was formational for Brett Conlon, CISO at American Century Investments.

After doing web development and data development during the dot.com era, Conlon moved to the U.S. Missile Defense Agency, where he was responsible for security servers and worked on program management. That led him to the FBI, where he spent 10 years working on national security and cyber defenses. In the private sector, he created the security program at Edelman Financial Services before moving several months ago to American Century.

“When I started in my career, I had the ability to work for some great leaders, and at the FBI had the good fortune to work with someone I consider to be one of the greatest mentors to work with,” Conlon recalled.

“He was very good at letting us fail, providing us top cover when we did. And he always told us to understand the business and not just develop or try to look at things from our lens, but the business lens and what we are trying to achieve.”

**Understanding the business**

In that case, the business was the FBI, but Conlon’s experience there provided a nice segue into private industry.

“**Understanding the business so we can provide the right type of security strategy is my business,**” he said. “**And so we develop the right risk tolerance and build innovation programs around that.**”

The biggest innovation he’s leading is redefining how risk is regarded, including explaining to the business side the added value that cybersecurity brings to the company’s bottom line, brand and reputation, he said.

He defines his role as “chief educator around all things security and risk, and making sure everyone understands it’s a company-wide responsibility.”
Risk and threat lens

“Part of our innovative strategy is making sure that everything we bring out really has that risk and threat lens on it already, and creating a way for our users to engage with us and our employees so they feel like they are part of the solution.”

Conlon is looking at department scorecards and individual scorecards so the business can now see the risks it’s bringing to the company, and what it can do to resolve those risks.

“That’s our unique approach to it, and it seems to be producing the correct conversations, producing the corrective actions that we want to see.”

One of the biggest challenges CISOs face right now is the very rapid pace at which the risk and threat landscape is evolving. It’s a challenge to keep up with that and build programs that are scalable and can help the business grow, Conlon said.

Cyber warfare

Malicious nation-state activity is on the rise, with cyber warfare playing out between Ukraine and Russia, Iran and Israel, and in China, he said.

“The pace at which that is evolving, and the pace at which risk and how we manage it is evolving provide a big challenge for us,” he said.

Supply chain risk is another challenge because there’s not a lot of transparency in supply chain risk management today, he said.

American Century is evolving continuous monitoring programs for third parties. It’s also looking at how frequently third parties are being evaluated and how risk rankings are given to third parties so it can figure out how to represent the risk correctly to the business, he said.

Continuing education

With the security landscape changing so rapidly, Conlon puts a premium on making sure his employees are continually growing and learning.

“It’s my job to make sure our team is as marketable as possible by continuing to develop, nurture and foster them in their educational pursuit of the ever-changing cybersecurity landscape,” he said.

That professional development creates a culture where they want to stay, he said. And while Conlon isn’t experiencing talent shortage problems, he thinks they could be mitigated industry-wide by loosening the requirements for candidates.

“We don’t really prescribe ourselves to X number of years of experience, or this type of cyber degree or master’s in computer science,” he said. “We’re really focused on the ability to learn, and how quick they pick up on things. The rest of it can be taught.”
Internship pipeline

The company also has built a strong internship pipeline to bring in talent, he said.

“With labor shortages, a connected workplace, and a landscape that is evolving at a rapid pace, I think it’s the CISO’s job to build out a very innovative, welcoming program that attracts talent and keeps that talent,” he said.

Another piece American Century does well is making sure that security isn’t kept behind the scenes, Conlon said.

“We do a really good job of making sure our employees are aware of it, that we’ve created an active engagement, and that the security team itself is very engaged in the different areas of the business,” he said.

Active mentor

Conlon is an active mentor. He works with aspiring cyber practitioners at the Air Force Academy, and at his kids’ school, he educates pupils about cyber safety and gives guidance to youngsters interested in getting into the industry.

He’s also created partnerships with local colleges and the police in the past, and is looking to establish those partnerships again in his new home in Naples, Florida.

After hours, Conlon volunteers as a soccer and flag football coach for his children, and does paddleboarding in the ocean. He also takes early morning walks.

“That helps me sort of catch up on my day, get my time to take a break from work itself, and just focus on the simple things.”
“Confrontation is not for everyone, but I feel that it’s necessary for you to grow,” she added. “If you’re doing everything and it’s not happening, well, maybe that’s not the right culture for you. It’s time to move on.”

“Is that your boyfriend’s computer?”

Laura Deaner has shaped her experience of such questions into a powerful message for underrepresented sectors in cybersecurity, persevere.

“Don’t get caught up in those moments where you feel like somebody’s making you feel like you don’t belong there,” said the CISO from Northwestern Mutual, who faced gender bias throughout her studies and career, as well as discrimination over her background as a North African with a Muslim family. “Whether it’s because of your gender, how you identify or even your cultural background, whatever you want to do, you’ve got to persevere and not let other people have that agency over you.”

The numbers have risen, but still today, only about one in every four CISOs is a woman. When Deaner began studying computer science at Old Dominion University, there were only five women among a class of roughly 300.

Seeking a community

“When I was younger, I probably didn’t have the confidence to address biases, so I found a community in employee resource groups,” she recalled. That setting allowed her to be authentic, without fear, and helped her to gain the confidence to confront a situation or person when she felt like they were biased.

Women in IT was an obvious group to join. Deaner also joined other employee resource groups that didn’t necessarily fit her background, like the Asian Employee Resource Group, to get different perspectives.

“I learn something every time,” she said. “I don’t care how many degrees I get or books I read, I feel like I get much better interaction when I’m actually hearing from the community themselves. That’s why I join every single employee resource group so that I can learn as much as possible. Over the last two companies I’ve been at, I had the fortunate opportunity to be part of the Diversity, Equity and Inclusion structure.”

‘Very isolated’

Deaner recalls being at a financial services company when 9/11 happened.

“I felt very isolated, because there was hate crimes against Muslim Americans at that time,” she said.

“And I unfortunately experienced some people saying some pretty bad things at work. Being involved in a community through an employee resource group helped me feel that I belonged, confirmed that what these people were saying was not OK, and gave me the resolve that I could do something about it. That touched me very early in my career, and that passion has been fueled over time as I became more involved.”

Personally, she can’t pinpoint a situation where she was passed over for promotion because she’s a woman, but she’s heard such stories. Her advice is to start with managerial conversations and hold them accountable to explaining why and where the development opportunities are.

“I’m very analytical, so I would want facts on why I was not the right candidate for that role,” she said. “Then have some empathy and be open to the possibility that there are things that you have to work on right now. You have to find out what behavior it is, or what capability you don’t possess. However if there are no facts, then I’m a fan of escalating. I’m also a New Yorker, so maybe that’s part of my direct nature!” she said, laughing.

“Confrontation is not for everyone, but I feel that it’s necessary for you to grow,” she added. “If you’re doing everything and it’s not happening, well, maybe that’s not the right culture for you. It’s time to move on.”

Business leader

In her current job, Deaner sees herself first and foremost as a business leader.

“This may be controversial, but cybersecurity and risk management is not just a technology thing,” she said. “It is something that may manifest itself in technology, but it is a business problem. That is why I see myself as a business leader. My role is to ensure that I’m setting strategy to ensure that we are not going to wind up on that headline — but also to make sure we have a world class and relevant cybersecurity and IT risk management program.”

With her background in technology, “there were plenty of times I just wanted to shut something down, but the business was going to be hurt by it. I needed a good mentor, or manager, to tell me that’s just not going to work, and you’re going to have to change your approach on that,” Deaner said. “The technology background helps, but the business side is super important because if you feel that everything gets solved by shutting something down, then your business is probably not going to like you all that much.”
Deaner devotes time explaining her program, or addressing something that might have been in the news, to others in her business and regulators, too.

“I spend a lot of time making sure my stakeholders – which is pretty much everyone, honestly – understand what we do and understand how that impacts the business, just breaking it down for them in a way that they can get it.”

The cybersecurity talent shortage is one reason she’s changed her philosophy on whether a cybersecurity team must be stacked with computer scientists or computer engineers.

“Now, I look for the capacity to learn and the capability to solve problems,” Deaner said. “The interview process to me is really important.”

“I also look for humility,” she added. “We are all really smart in technology, and I think practicing some empathy is going to go a lot longer than being lectured about something that is not working properly. Listening to another group of people and understanding what the problems are, taking other perspectives, is really important, so I look for that as well.”

As a computer scientist, Deaner has always been fascinated by artificial intelligence, so she’s interested in applying AI and any kind of machine learning to solving tough problems in cybersecurity. However, cybersecurity is an industry that has exploded with solutions, and teams have to do their research to separate the hype from the facts, she said.

“What’s important for me and my team is actually looking under the hood to understand what’s really happening, by asking really great questions. We get a lot of vendors that want to send us PowerPoint slideshows and we don’t even look at them. Instead, we get on a call with them and ask them to tell us technically how they’re doing this thing or that. We glean a lot more information doing it that way than getting a demo or seeing a 60-page slide deck of how great they are and how many other companies are using them.”

Maintaining a good work-life balance – or work-life harmony, as she puts it – is a constant challenge.

“I have to remind myself and keep disciplined every day that my mental health is important to me. My family is important to me,” said Deaner, the mother of four young children. “I put in boundaries about five years ago, but I have to reinforce them constantly, because otherwise, I’ll be sitting here in this beautiful NYC office until midnight working.”

When she unwinds, it’s with her family. They love to get outdoors to bike, hike, and go to the beach or pool, she said.

“I personally love astronomy because I’m a big nerd,” Deaner said, laughing. “I love reading about the James Webb Space Telescope. I try to get out and look at the stars as much as possible, but living in New York City makes that challenging. We try to go upstate as a family where there’s not a lot of pollution and just look up.”

“I’m still working on my kids to see if they can be as nerdy as I am on this stuff, but they’re not there yet,” she said with a chuckle.
Mark Eggleston came to cyber security from a career in psychotherapy, and he’s brought that people-centric experience firmly into the C-suite.

“What I like to do is value the interpersonal contributions of each person, and make sure we’ve got a diverse program to cover diverse needs,” said Eggleston, the CISO of CSC, a provider of tax, legal, digital protection and branding services.

“It’s often said you have three resources: people, process and technology. I really believe in following that order. Sometimes you want to go after the first great technology. But that shouldn’t be the first course of action, which should instead be how to recruit and retain.”

Cyber security is actually Eggleston’s third career. He graduated from college in the early 1990s with a bachelor’s degree in psychology, but there was a recession in full swing, so he worked in construction.

Stronger family support

Before long, he went back to school to get a master’s degree in clinical social work. Working with children and adolescents with physical and mental health issues was “wonderful, and very intrinsically fulfilling,” but when it came time to have a family, he wanted to expand his horizons and get other avenues for stronger family support.

His wife suggested he “do that computer thing you were thinking about,” so he went back to school for a post-baccalaureate in management information systems. For many years, he combined his clinical and business skills, first working for a company that did all the continued stay approvals for children across the state of Virginia in therapeutic foster care and residential treatment.

From there, he transitioned to a large hospital system, Catholic Health Initiatives, to help build its national privacy and security program, following the passage of federal health information privacy regulations known as HIPAA.

“I really found it interesting, both from the vantage point of an ex-psychotherapist who always valued privacy, and the administrative, physical and technical controls for security,” Eggleston said. “Being named a HIPAA security official was a begrudging task because typically you were given very little guidance, and people would always joke, ‘Hope you look good in orange ‘cuz you’re going to jail, you know.’”

His next job was with a regional HMO in Pennsylvania, Health Partners Plans, designing its privacy, security and business continuity program. He worked there 17 years until transitioning last summer to CSC.

“It was a wonderful opportunity, a kind of Great Resignation thing after 17 years at one employer,” Eggleston said. “It’s a global organization and has an optimistic and bright financial future. It’s very exciting for me to take on, and I’m using all my past experiences there as well.”
Transferable skills

“When you’re in construction, building things, you learn to roll up your sleeves and get dirty, and lead teams in the sometimes grudging work that security can sometimes be,” he added. “And the psychotherapist in me is doing that piece where you get to understand what motivates people, which is definitely a big piece of management. So I still use those different skills in what I do today.”

It was odd changing to a new job after such a long time in another organization where he held various roles and felt “immense comfort” with executive leaders and the teams he built, Eggleston said.

“The biggest challenge here was learning a global organization and an industry outside healthcare. It was interesting to get up to speed on that,” he said. “But security, the controls, the people aspects, the program, the technologies, they’re still all the same. So I latched on for comfort to some of those things that were the same, while pushing myself to embrace the uncomfortable.”

At the year-plus mark, Eggleston wants to make more global changes and efficiencies.

“I hope I’ve earned that latitude with my directs to push them differently,” he said. “So we’re going to continue to call each other out on things and continue to just get stronger together, so I think that’s the next challenge. But I’m sure we will rise to the occasion here.”

When he first started as a CISO, his core function was limiting risk. Now, he sees it as empowering business growth. “That’s a continual journey in conversations with the executive leadership and the board, probing risk tolerance,” he said.

Time crunch

At the same time, there’s no quenching of the thirst for new technology, and it’s a big challenge trying to select the best vendor, he said. A colleague once gave him solid advice: Get new entrants in the market and work with them to develop the product to meet your requirements.

“There aren’t enough hours in the day to vet all the new entrants into the cybersecurity market for technology and some of the process pieces,” he said. “I’m a big fan of getting more aggregate solutions under a single pane of glass and hopefully getting a shorter list of MSPs or valued partners to help us do this so we can work on maximizing that relationship and help them understand our culture and priorities instead of training a new vendor or a new managed service provider every year,” he said.

In the future, this onetime chief privacy protector expects to see more aggregation of the cyber security and privacy roles.

“I do think that we all need to continue building in privacy impact assessments into our security, making sure we’re looking at privacy, just using the minimum necessary information and making sure that the privacy of our consumers and employees is respected when we enable process and technology,” Eggleston said. “That’s a key trend and I think it will continue, becoming more science- and psychology metric-based, especially as it relates to providing cyber education to your workforce.”
Giving back

Eggleston describes himself as “a huge bourbon fan” who “likes to imbibe responsibly.” He also likes to boat and mountain bike.

“Both of those things are also ways that I help deal with mental health,” he said. “Unless there’s a core project, I typically don’t focus a ton on work on the weekend. That’s more about spending time with my wife and three children. In the evenings, it’s usually some work, at least a couple of nights a week. And I also do some side projects, whether it’s side consulting, or mentoring other folks, or just dialogue on LinkedIn.

“Although I’m not a huge social media fan, I’ve gotten a lot of guidance from LinkedIn, and now I like to give back a little bit more on that platform.”
ERIK HART
CUSHMAN & WAKEFIELD CISO
Erik Hart spent half of his career in financial institutions and the rest in organizations where clients played a larger role in driving security parameters.

One takeaway from his diverse experience is that cyber professionals have to learn they cannot be the “Department of No,” said Hart, today the chief information security officer at global real estate services firm Cushman & Wakefield.

“If you go in all the time, saying ‘No,’” or taking the black and white security mentality, unless you’re in an organization like a financial institution where you can take a much harder line, you’re going to fail,” he said.

“We’re trying to find a solution or path for our teams. I told my people, ‘All of you are supposed to be architects and solution engineers. How do we find a way to say ‘Yes,’ or say, ‘If we do this, here’s the risk and are we willing to accept that?’ and make the business think about those risks.”

Delegating responsibility

A good CISO will know how to communicate, and how to build relationships across different business unit lines, he said. A good CISO will also know how to delegate responsibility.

“How do you empower your team to make more decisions?” he said. “That’s something that’s been very hard for me. I’m an only child, so I’ve grown up with a lot of times, everything is mine. So I’m working on breaking away.”

Hart has been in the information security space for over 20 years, first in financial institutions, and then in trading and advertising technology before joining Cushman & Wakefield.

“The first half of my career was spent in the highly regulated financial institution space, where regulators and SOCs were major drivers for security operations. You did it because they asked for it,” Hart recalled.

As he moved on to other fields, “the focus shifted to finding the right solutions for clients. And since you can’t do one-offs for each and every client, it became about finding commonalities but also the various add-ons that you need to service clients or the business you’re working for,” he said.
Client demands

In his current role, responsibilities entail all of global security, including risk management, information technology controls, governance, client and data security, technical security and some interim CTO responsibilities while his expanding company undergoes some reorganization.

The company has grown from 40,000 people when he came on four years ago to more than 51,000 today. And more security demands are coming from the client side. So the No. 1 challenge has become, “How are we building out security into the sales cycle, especially with people in the commercial real estate services space who are not technology-driven, but whose services are driven by technology?” he said.

Another challenge is the numerous third parties the company uses, both in terms of SaaS systems and contractors, consultants and other suppliers. Cushman & Wakefield is addressing this risk in part by putting more and more things attached to a single sign-on “so we can drive and own the identities,” he said.

“Third-party vendor-risk management is something we all deal with and everybody does it in a different way,” he said. “It’s one of those areas that’s ripe for disruption, but I don’t know if we’ll ever get enough organizations coming together on a common way, setting an ISO-type standard to assess and deliver that,” he said, citing cost as one obstacle.

Uniqueness and diversity

The last big challenge is bound up with the technical uniqueness and diversity that comes with a global organization, where different countries have differing and sometimes conflicting rules and regulations, he said.

“That’s been a challenge,” he said. “How do you have a unified security approach when you have various country or regional rules and regulations?”

Hart sees the industry heading in a direction where identity becomes the centerpiece.

“Security and computing in general is moving past that hardware stage where you’re buying pieces of equipment that have blinky lights that you put in a rack somewhere, and we’re really moving to services,” he said. “So for us, it’s not about firewalls anymore. It’s about identity, because many employees can technically pivot to various devices to do their jobs. How do you deal with identity rights? How do you build a lot of the security controls into identities and not necessarily care about the devices people are using to do their jobs?

“I’ve also pushed over time to get out of assets management, i.e., issuing laptops, in favor of putting the security around the identity and what people access,” he added. “I don’t care what computer they use. If you want to send them a computer, fine, but if we want to get out of the supply chain nightmare, can we have them use what they already have? That’s where I would love to see things go.”
Vendor consolidation

He also sees more of a push toward automation and outsourcing, and consolidation in the security vendor space.

“I want to consolidate and have things be good enough but operationalize them well, versus buy a bunch of best-in-breed products that my people can’t operationalize because there are 10 or 12 things going on at once,” he said. “I think you’re going to continue to see a little bit of that consolidation around certain bigger vendors who are making the investments in the industry.”

When he’s not shielding Cushman & Wakefield from bad guys, Hart is likely to be found toiling in his yard.

“I bought a house almost two years ago, and it has two acres of property. I refuse to pay somebody to mow the lawns, so I spend anywhere from four to six hours on a summer weekend doing various yard work,” he said.

He’s also an avid Peloton rider.

“I’m on the bike almost every morning. So those are the ways I try to do it, to get away from the technology and not look at a computer,” he said.
MATT LEMON

HUAWEI MOBILE SERVICES CISO
Matt Lemon, the Chief Information Security Officer at China-based Huawei Mobile Services, comes from an extremely technical background. He has a master’s degree in computer science from MIT, and a doctorate in cyber/computer forensics and counterterrorism.

He also thinks it’s important for CISOs to have a broad range of experience so they can understand enough about the technicalities.

But what he’s always subscribed to is to hire smart people and let them do their jobs.

“I don’t get involved in their day to day duties. I let them go on with it because they were hired because they’re good at what they do,” Lemon said. “My role is more to set the strategy and to look after the personal and professional development of all those people that I’ve hired.”

Emerging from the pandemic, CISOs have had to learn a whole new set of skills because they’ve had to be a lot more empathic with the teams they manage because people have been sick or had issues working from home.

“The ability to support your team at a personal level is something that I think is definitely a requirement for CISOs now,” Lemon said. “Another thing that we probably over the last few years have gotten to grips with is the fact that security isn’t a siloed operation. We need to be good at building relationships with different stakeholders, whether that’s finance, marketing, HR, whoever. They all have security concerns, and they don’t necessarily bring those to you unless there’s a trusted relationship there.”

Lemon’s been working in the industry for 25 years. Today, a CISO’s role is really more of a business one, to make things as secure as they need to be rather than as secure as possible, he said.

“Everybody wants things to be secure, but you can just keep throwing money and time at security endlessly, almost,” he said. “You need to be aware of what the business goals are and what their risk tolerance is so that you can define your security plan accordingly.”

At Huawei, where he’s been for three years, he’s built a team pretty much from scratch. On the sidelines, he’s studied Chinese and done a law degree.
‘It’s useful having the degree, looking at contracts and data privacy and that kind of stuff,’ he said. ‘It’s a big advantage for me in this role.’

Before Huawei, Lemon was chief information security officer at Ulster Bank, and CISO for SaaS cloud security and a partner in the cloud security practice at IBM. He served as chief information security officer for the government of Ireland in the late aughts, and afterward was one of the pioneers in providing managed security services.

‘Security was really just in its infancy,’ he said. ‘The smartphone had come out and things were just being connected. People were scrambling to try to find anybody that knew anything about security to hire them.’

Lemon commands a team of about 700 people. His biggest challenge now is recruitment.

‘It’s almost impossible to get experienced people,’ he said. It’s easy to get people straight out of college, but they don’t have the experience and the knowledge to step straight into a role and contribute from the start. They need six months of handholding and mentoring before they become productive.

Retention is another problem because of the talent shortage, he said. ‘I could offer somebody $100,000 to do a job, and then after six months time, somebody else is going to offer them $150,000 to work somewhere else.’

The lack of qualified staff is driving a big push toward automation, Lemon said.

‘We’re trying to automate as much as we can,’ he said. ‘We’re especially concerned with fraud prevention, both financial fraud and fraud using our customers’ accounts. So we are spending a lot of time and effort in getting up to speed with artificial intelligence and machine learning so that we can automate as much as possible the detection of fraud and any anomalous activity.’

After a number of years where budgets weren’t hard to come by, spending is now being cut or frozen industrywide.

‘Because money is under more scrutiny, it forces people to become more innovative in the jobs that they’re doing and the tools that they’re trying to use,’ Lemon said. ‘If we can’t get approval for a particular project or a tool, then it makes people think whether we can repurpose something that we already have to do something it wasn’t necessarily designed to do.’

**His advice to younger CISOs: Try and get the broadest understanding of all the domains of IT so you can help your team with personal and professional development.**

Ransomware is one of the external attack threats that his teams spends the most time on. ‘We’re not so concerned as we used to be about the iconic kid in the basement, in the dark, hacking away,’ Lemon said. ‘We’re more concerned with state-sponsored attacks and ransomware attacks than anything else.’

‘I spend quite a bit of time having one-to-ones with not only my direct reports, but their direct reports as well. I probably spend 50% of my time in meetings like that.’
Lemon lives in the countryside outside Dublin. There are forests on his doorstep, so he likes to go walking. Because of the large amount of travel he used to do and the commuting, he’s gotten into audio books.

He also keeps two donkeys, Clinton and Cobham.

“When we moved into the house that we’re in now, there was about an acre and a half of field that was seven feet high, really tall grass and brambles. So we got two donkeys from a local rescue center.

“They’re great, real characters,” he said. “I can go in the field and chill there with the donkeys.”
TOMÁS MALDONADO
NATIONAL FOOTBALL LEAGUE CISOS
MARCH 2023
CISOs CONNECT MAGAZINE | 39
A desire to grow is the overarching principle that has shaped Tomas Maldonado’s career.

Maldonado, the CISO of the National Football League, has been in the profession for about 25 years. He trained in university as a computer scientist, but decided he didn’t want to be a programmer. So as the internet evolved, he decided to take more networking classes.

He “stumbled into” information security at Schroders, a small investment bank, after they advertised for a network security officer and trained him.

“I knew the network angle, but I didn’t have the skillset of what is known as cybersecurity. The company allowed me to learn and grow,” he said.

’Grew up’

In 11 years at Goldman Sachs, he “grew up,” starting off as a hands-on technical cybersecurity person, then moving up the ranks to vice president, where he built the company’s first data-loss prevention program.

He moved to JPMorgan Chase “to grow my leadership and management style.” He served as the Chief Information Security Officer for the Corporate Technology & Risk line of business, and after four years there, left for chemical manufacturer International Flavor and Fragrances to be in a capacity where he would report to the board and step outside information technology.

The combination of working in financial services, where he learned and refined cybersecurity skills and controls in a highly regulated industry, and working in a very creative company like IFF, “prepared me for where I am today, at the NFL, running its security program,” he said. He’s been there three years.

Most viewed

Maldonado’s work at the NFL, where he provides cybersecurity services for the league’s clubs and stadiums, is different from prior experiences, he said. For one thing, the Super Bowl is the most viewed sporting event in the world.
“Our product is our sport,” he said. “The NFL being a high-profile brand, and the Super Bowl being the most-watched show in the world, we have to meticulously prepare as cyber attacks in all environments proliferate.”

**Biggest influence**

The different opportunities and different industries have influenced him more than the CISO world, Maldonado said.

“The security and technical aspects I grew up learning influenced me along the lines of seeing where technology is shifting and moving,” he said. “But adapting to different industries and learning what motivates them is more fascinating to me.

“I really like the fact that I’ve been able to travel with these opportunities, and meet people in different countries,” he said. “What I’ve found in that travel is that there is a lot more that connects us and binds us as people than separates us. That’s been very rewarding. It’s allowed me to be more flexible and more thoughtful in how I implement my security program.”

**Helping colleagues**

It’s also important for Maldonado to help colleagues grow. With other peers, he hosts thought leaders on a weekly podcast to share their origin stories. “It’s a way to help provide mentorship ‘in bulk’ by leveraging our platform, he said.

He’s served on advisory boards for several companies, helping to shape the next generation of security solutions to meet business use cases. He is currently co-chair of Evanta’s New York CISO group, and is an active member of Security Current, he’s hosted its Security Shark Tank event.

**Deepfake threat**

One thing that’s very top of the mind for Maldonado is the emerging risk around deep fake technology, where existing video or images are manipulated to insert someone else’s likeness.

“We have very public celebrity-type people with a lot of footage on them, and you could easily create a video of one of the players, or any one of the coaches or any one of the NFL senior executives and use that for something malicious,” Maldonado said. “So trying to find creative ways to mitigate that particular risk, and working with companies that are looking to protect against that risk is very near and dear to my heart. It’s more apparent in this industry than prior industries I’ve worked at.”

**Keeping cool**

Being calm under crisis is probably the most significant contributor to a CISO’s professional success, Maldonado said.

“You’ve got to be a good listener to be a good leader. You need patience. But being calm under crisis is probably the most important trait, because people look to us to be that calming factor for them,” he said. “Whenever you have an incident, people are looking to you to be decisive, to be that leader, to be that coordinator, to be that calming voice in the midst of all of the chaos,” he said. “If you’re not able to exercise that level of calmness under that level of stress, it will be challenging for you.”
Different adversaries

To unwind, Maldonado tries to spend as much time as possible with his family, and he likes to travel. His last personal trip was to Hawaii, where he went right after the Super Bowl to decompress, and he’s interested in traveling to the Seychelles or Maldives.

“I need some sand between my toes, a nice, cold beverage in my hand, and the sun just beaming on my body,” he said.

He also enjoys scuba diving.

“Nobody can reach me underneath the water on my mobile phone or any other electronic device,” he said. “When you’re underwater, you’re there for how long you can be there and nobody can touch you. You’ve got sharks and other stuff, but those are different types of adversaries.”
Kevin Morrison has worked in a variety of industries, each with its own unique opportunities and challenges, but all converging in one overarching principle: the need to build relationships.

“My career path has influenced my CISO role by really understanding the criticality of the partnerships that need to exist, regardless of the industry,” said Morrison, who recently joined Driven Brands, an automotive services company, as its first cybersecurity chief.

“It’s driven home the need to proactively reach out to folks across the business to really build those relationships, to understand how the security team and function can really support what needs to get done, and to make sure we’re in alignment with the roadmaps that are being developed.”

**Business MBA**

Morrison did his bachelor’s degree in information technology, and started his career there before gravitating toward cybersecurity around two decades ago at a time when there were a lot of disruptive viruses.

Building on his rich technical background, he did an MBA in technology and innovation management to better understand the business side of things. “Each station has been a great stepping stone and opportunity to take on broader leadership roles and eventually becoming a CISO at a couple of different Fortune 500 companies,” he said.

Morrison’s work history spans industries including defense-related engineering, law, homebuilding, aviation and most recently, after-market auto services. He joined Alaska Airlines at the start of the pandemic, just as carriers were being clobbered by a sudden near-halt in travel. But because he was confident in their fiscally conservative stance, he joined the team.

“Had it been any other airline to come on to that role in the midst of a pandemic, I would have turned it down,” he said.
Increased scrutiny

Driven Brands brought on Morrison in June, roughly a year after it went public -- a development that created increased scrutiny of its business processes and the need to put in place the right controls to manage risk. Part of his challenge is to change the business culture so everybody within the organization understands that security is everyone’s job and is an opportunity to help protect the brand and revenue by minimizing incident-related costs.

Engagement across the organization is critical, he said.

“Any time you’re coming into a new role, especially where you’re the first one in that position, right out of the gate you have to ensure that people within the business understand what you’re there to do,” Morrison said. “You also have to make sure that others know how and when to reach out for guidance on risk management, and that it’s not just me or my team in a bubble making decisions.”

Alignment is key

In an early CISO posting, Morrison had the good fortune of receiving management’s support for most of the investments he sought. What he didn’t consider then was that his program didn’t exist in some kind of splendid isolation.

He didn’t engage with peers over their respective areas, and when it came time to execute on solutions his team was moving forward with, they weren’t aligned on resourcing and prioritization with other teams they relied on for implementation.

“That definitely helped me better understand right out of the gate that I have to go in and engage my peers as early as possible, and as often as possible, to make sure that we’re aligned on where I see the gaps, and that we have the appropriate resources to go in and do the implementation and ongoing maintenance,” he said.

“I can’t overemphasize enough how critical those relationships are for peers and for business stakeholders, to understand that you are there to provide a service and to partner with them in securing the organization.”

Ditch geekspeak

The CISO’s role has evolved from very technically focused to a greater focus on the business, and communication has been key to those who have been successful in this transition, he said.

“It’s so important for them to be seeing you as somebody who they know they can proactively reach out to and have a normal conversation with instead of geekspeak that’s going to make them roll their eyes and look like a deer in headlights,” he said.

Morrison’s overriding philosophy is to try to minimize friction. Most of the controls that he’s deploying aren’t creating a lot of visible change that will require employees to redo workflows. As a result, he’s a big fan of continuous attack path analysis platforms.

These highly technical tools run in the background, so aren’t disruptive for colleagues. But they provide CISOs the opportunity to have a more business-driven discussion with executive stakeholders and the board about how security-related investments are working or aren’t living up to their marketing hype, he said.
“CISOs have been challenged over the years to really provide quantitative evidence showing the value of the investments we make and the efficacy of the controls that have been deployed,” he said. “With this particular platform, we can 24/7/365 run simulated attacks based on hundreds of pre-canned attack vectors, which allows us to determine the exploit potential for an attacker to gain access to the environment, and then pivot from there.

“Having the ability to say with confidence that we have the appropriate controls in place, or know we've got a glaring hole and need to deploy a new configuration or new change or new technology – that continuous visibility is critical.”

Another key thing Morrison is doing to minimize friction is revisiting the authentication space. Instead of requiring everyone to change their 12-character passwords every 90 days, he's now a fan of less frequent password changes, following NIST guidance for a higher number of characters, but less complexity.

“Removing complexity means fewer employees who forget their passwords because they don't remember if it was an exclamation point or a pound sign or whatever,” he said. “It's a win-win. You're improving the risk posture of the organization while minimizing the friction. Looking for opportunities around those types of areas definitely can be a win.”

**Tee up**

Golfing and music are Morrison’s chief outlets for unwinding.

He and his family live on a golf course and he plays at least a couple of times a week. He grew up in a musical household, and to the dismay of his family, he quips, he started first on drums.

“I now have a nice electric kit, and can plug my headphones in and not bug anybody,” Morrison said. “I play guitar and a little bit of piano as well, so I really enjoy it in my own time, just to unwind and have that outlet. I have such an eclectic taste in music, it's all over the map. You name it, and I'll most likely be into it.”
Growing up in the Dominican Republic with limited means has had a big impact on Yonesy Núñez’s career and the way he sees his role.

“When you have limited resources, you become very resourceful at figuring out how to move forward, how to strive,” said Núñez, the CISO at fintech company Jack Henry. “I’ve always been a person who wants to take things apart and figure out how to make them better.”

These austerity-driven lessons stay with him today, at a time when money and cybersecurity talent are tight. Limitations can be worked around with the right approach, he said.

“Limitations are really about helping people understand what the problem is and its potential impacts,” he said. “Once they understand that, learning how to work around those limitations is part of the job. I don’t find there are limitations when you’ve prioritized activities, whether you’re managing a $2 million budget or a $2 billion budget.”

**Technology crush**

At age 12, Núñez emigrated with his family to the U.S., where he quickly became enamored with technology.

“I was always amazed that there was so much inside such a small device that you could interact with, and bring to life,” he said.

After college, he worked as network administrator and director at New York Media Group. He got into security after attending a 1997 conference on security and management.

“The internet was nascent at that time, but I understood that once it would become pervasive, we were going to be under siege,” he said. “I came back and said to my boss, ‘We need to get somebody here to protect us.’ He turned around in his leather chair and said, ‘You’re going to do it.’”

**Got messages across**

Núñez got his first big CISO job at a global manufacturing firm, Pall Corporation, after he gave a talk at a conference.

“The CIO came up to me and said, ‘Normally, I can’t understand what you guys say but I understood everything you said. I want to hire you,’” he recalled.

“I learned a lot in that role about different cultures, the global landscape, people and their differences, and how we’re basically all the same, just different points of view depending on what our culture shows us and what we learn from it as we grow,” Núñez said.

His frequent trips to Japan spurred him to learn martial arts. He also picked up the language.

“Going to Asia as an Afro-Latino at that time was really hard,” he said. “The best thing you could do is try to speak the language.”

**Doctoral studies**

While at Pall, he also completed his doctorate in computing and information security.

Núñez pivoted to financial services after a fellow speaker on a panel told him financial services “is where the battle is being fought.” After a year and a half as manager for Practice Leader Risk and Security Assurance at PWC, Citigroup came knocking. Wells Fargo followed shortly after.

Over time, Núñez came to understand that the job is not only about understanding cybersecurity, but also about helping to take the company and its customers forward.

“You’re not just protecting the environment, you’re using security as a differentiator,” he said.

“One of the things that drew me to Jack Henry was the drive to make sure that community financial institutions remain competitive in this space. Community financials are the lifeblood of America, and it’s really exciting for me to do what I do to help in this space, always striving for positive outcomes.”
Transformational role

The CISO’s job has expanded beyond security to become a transformational role, Núñez said.

“COVID accelerated digital transformation for all companies, and the CISO is probably best positioned to help with that digital transformation by understanding how technology works and what is within the realm of possibility to help organizations remain competitive and succeed,” he said.

The main trait he thinks a successful CISO has to exhibit doesn’t involve technology, however.

“Empathy is probably the biggest thing, not just for cybersecurity, but for being a leader,” he said. “It behooves you to empathize with your constituents, customers and peers, and the folks in the world around you. Understand their stories.”

Methodology focus

One prominent feature about Núñez’s approach to his job is the focus on methodology.

“Endeavor to continuously modernize the approach to cybersecurity,” he said. “Shake things up within your teams to start honing in on new attack patterns, vectors, or new technologies. Remove the fanaticism about tools and processes, focus more on solving problems, and develop teams that solve the problems, rather than focusing on the tools.”

Building a roadmap is essential, he added.

“Many leaders across the board don’t really take the time to understand the current state, map out where they want to go, and align that with the business and their customers,” he said. “Bringing those elements into the program helps build a strong following and a passionate team. They’ll be more mission-driven, and I think that’s something that we ought to bring to the table more often.”
Automated attacks

Faster and more automated attacks are the biggest trend the industry has to deal with now, he said.

“Sometimes we think that there is an attacker, a person, coming after us, but 99 percent of the time these are bots that we’re contending with,” he said. “It’s an asymmetric battle with humans fighting machines. Humans get tired, machines don’t. We need a better defense system. 24/7 automation is what’s really going to help with that process,” and automation is a major innovation he’s bringing into his company.

Aside from practicing martial arts, Núñez likes to watch sports – basketball, football and baseball. For a long time, he also built and raced cars, and he still has one car left. “It’s that tinkering,” he said. “How much more performance can we squeeze out of this machine?”

Giving back

Giving back was always a priority, and during his years at Pall, he built a cybersecurity program for Mercy College in the Bronx. He also taught several classes there. One of his passions is to help the next generation of women and minorities in cybersecurity, and he has been mentoring and advocating in this space since 2005.

“‘It’s a little grain of sand because I can’t mentor the world, but I think it’s important. We have a saying in the Dominican Republic: poquito a poquito se llena la jarra – little by little, the jar is filled,” Núñez said. “Seeing them see things the same way and pay it forward, that for me is the best feeling in the world. I will keep working on filling the jar.”
“We need to pay attention to people who may not have a cybersecurity or information security background,” she said. “We as leaders need to identify other talents and/or experience and soft skills they possess and recognize how that could be of value for our programs or roles we’re looking to fill.”

Coming up from help desks, the ground floor in IT, gave Elizabeth Ogunti, the CISO at JBT Technologies, a greater understanding for what the IT team as a whole experiences. It’s also made her ardently determined to bridge the communication gap between IT and the rest of her company’s business.

“My biggest challenge is making sure that leadership understands the value of the IT environment, including what it takes to secure it,” said Ogunti, whose company provides technology solutions to the food processing and air transportation industries.

“Data security comes with the territory. But one of my missions is to help the organization as a whole gain a security mindset. Realizing that each team member plays an important role in maintaining a secure JBT environment and providing education about the importance of practicing safe data handling.”

In her current role, Ogunti is trying to introduce several innovations, including network segmentation and a new approach to passwords, possibly through password managers or a passwordless environment altogether. She’s also weighing increased usage of Microsoft tools.

In an age of budget constraints, Ogunti said she tries to be thoughtful in her request for tools.

“When I first arrived at JBT nearly seven years ago, I did mapping exercises for controls and the policies and tools we had in place. And then I documented the deficiencies and made a roadmap to mitigate risk,” she said.

“I review the roadmap annually to determine what’s next. I don’t ask for a bunch of stuff every year. I tell my team to talk to vendors to see if we are using tools to maximum benefit. And I work with our managed service providers to get the most out of our contract. And then I take a look to see what’s next. I think by doing that it puts you in a better place toward understanding your network, environment, and risk mitigation so when those constraints come, you can be in a good place.”

Ogunti is a big advocate of hiring from within. Her current team started out as a person of one. Over time, she’s brought on three more people with varying backgrounds – for types of jobs they didn’t perform before.

“We need to pay attention to people who may not have a cybersecurity or information security background,” she said. “We as leaders need to identify other talents and/or experience and soft skills they possess and recognize how that could be of value for our programs or roles we’re looking to fill.”

She urges cyber professionals not to feel pigeonholed into any single area.

“Cybersecurity is a broad field,” she said “There are so many areas that folks can get into that require a varied skill set.”

Ogunti, a 10-year veteran of the Army military police, went to school for programming. She intended to be a C++ programmer, but when she was job-hunting, an opportunity to join EDS and work in a Windows environment opened. It’s something she didn’t have experience with at the time, but mentors, she said, “helped me get up to speed.”

She did network administration there and at FMC Technologies – a founding company of JBT – where she later become an auditor for Sarbanes-Oxley compliance. She was a special projects IT auditor at RWC, an information security program analyst at BMO Harris Bank, and at JBT, she started out as a contract IT SOX auditor before working her way up to CISO in November 2020.

Ogunti expects the CISO role to expand exponentially over the next couple of years, with more involvement in the boardroom.

“Cybersecurity is now the main focus for everyone,” she said. “As more organizations’ leadership realize this, they’re going to want to have someone on their team who understands security and how the organization is performing and mitigating risk.”
“You also have regulatory changes that are taking place,” she added. “The Department of Defense has a whole certification process for businesses that want to do contractual work with them. And the Security and Exchange Commission is going to put more responsibility on board members to understand cybersecurity in their organizations. Our role is going to increase and take on more value.”

A successful CISO, Ogunti said, needs to be an effective communicator with both the IT sector and on the business side, in order to convey risk and security issues to business professionals who don’t understand IT lingo.

“I also think CISOs need to be open and relatable. Because security affects everyone, not only in the office, but at home. So if you want cooperation, you need to be approachable,” she said.

The CISO title, she said, “doesn’t put me on any different level in my mind.”

“To me, I’m still part of the help desk. I’m still a part of the IT people,” Ogunti said. “I think that lends to my credibility as a CISO, because I understand IT.”

Outside the office, Ogunti serves on the board of the Unity Parenting and Counseling, an organization that helps at-risk youth, as well as foster and homeless families. She is an Associate Board member of the Union League Boys and Girls Club as well.

To unwind, she crochets—something she picked back up during the Covid-19 pandemic. She likes to binge-watch TV shows like Ozark, reads spy novels and history books, trains her Cane Corso, and hangs out with family.

She also does a lot of dancing, of all different types. “Dancing is something I really enjoy,” she said.
“You have to listen to your business partners. We’re here doing cybersecurity and risk management because of the business. Hear them, listen to them and find a collaborative path forward.”

Learning the business.

That’s the direction in which a CISO’s role is evolving, says David Ortiz, the cybersecurity chief at Church & Dwight, the maker of Arm & Hammer products and other household goods.

“You’ve got to know all facets of the business, understand the risk of them, and put together the right roadmap to reduce risk,” Ortiz said.

Today, resilience and identity and access management are top priorities, he said. At Church & Dwight, he’s focusing on an ironclad cybersecurity incident response plan that works in harmony with business continuity plans, disaster recovery plans and crisis communication plans.

As for access control, “We’re making sure that our people only have access to what they need.”

Collaborative path

At the same time, cybersecurity chiefs have to understand that they can’t be deploying security for security’s sake. That’s where learning the business comes in.

“If you’re in the private sector, you can’t be an impediment to driving revenue by putting too much protection in place that the company can’t do its job,” he said.

“You have to listen to your business partners. We’re here doing cybersecurity and risk management because of the business. Hear them, listen to them and find a collaborative path forward.”

Ortiz’s career history began with a degree in computer science that took him to consulting assignments on application development at New York City brokerage houses. From there he moved on to retail and publishing companies, spending 20 years at Bed Bath & Beyond before arriving at Church & Dwight two years ago.

Always security

“Security was always part of what I did and what everybody did, but we didn’t really call it security. It was part of the build and development process,” he said.

“When I really raised my hand and got involved was when payment card compliance became mainstream and companies needed to start adopting stricter compliance on the IT and the IT security side.”

Initially, as he formalized Bed Bath & Beyond’s cybersecurity department, things were still very technically focused. Several years later, he started breaking off from information technology, and set out to transform things again.

“I wanted to make the Information Security department more of a business-facing department to interface with our business leaders, and really develop the information security department more as a business function than an IT function,” he said.

Ortiz connected with Church & Dwight at the early stage in its security program, and over the past few years, has significantly increased its cybersecurity maturity, he said.

Persistence and time

“There is a lot of persistence that’s needed for the role,” he said. “I’ve been fortunate to have great teams at both organizations,” he said. “Self-education and persistence have helped to foster a good team environment, and foster the right next step forward for the company so cybersecurity is really embedded in the culture.”

One of Ortiz’s biggest challenges is time.

“We run out of time every day,” he said. “Everybody is working really hard, and we need time to get our roadmap accomplished. But we also need that right work-life balance, and let people take a break and get back to their personal lives and decompress.”
“Be prepared to be a constant student. And be prepared to collaborate,” he said. “It’s a wonderful industry and everybody’s willing to help one another. Be prepared to get involved. It’s a profession. It’s a career. It’s a lifestyle.”

“Bad actors only have to be right once,” he said. “We have to be right every single time. It’s a hard balance to strike, and sometimes people take that personally. Teams need to know they have our support, and that we’re going to help each other to move the ball forward.”

Because time is such a major constraint, Ortiz looks to find time-saving technology. But at the end of the day, “I don’t really want to start with a technical solution,” he said.

“I want to start with the process, and an understanding of the risk, goals and the outcome. I always find myself going back to the same thing: Let’s have a strong foundation and make sure everyone understands how to keep that foundation strong by doing what seem like basic things but do them really well.”

With budgets limited, Ortiz takes a risk-based approach that assesses what presents the organization and its people with the most risk and how his team can reduce it. But flexibility is also key.

“We can’t say on January 1st that we’re going to do something for the next 12 months;” he said. “It’s a constant re-evaluation of the external threat landscape and risk, and adjusting the roadmap for that.”

For those entering the profession, it’s important to understand that this is not a 9 to 5 job, Ortiz said.

“Be prepared to be a constant student. And be prepared to collaborate,” he said. “It’s a wonderful industry and everybody’s willing to help one another. Be prepared to get involved. It’s a profession. It’s a career. It’s a lifestyle.”

When Ortiz does turn his attention elsewhere, he’s got two kids in college and a third right behind them. “I spend time with my family; that’s how I unwind, as much time as I can with my family and friends.”
“As an educator, we are trained that if you want to be effective, you have to know how to speak to your audience. As a CISO, I have multiple audiences, and I need to speak to each of them in language they can understand, that resonates with them – same as I do with my students.”

In the course of a 26-year career, Garrett Smiley has ping-ponged between technology-focused and educational roles, on top of getting an infosec-related PhD. That dual focus has colored how he approaches his CISO job.

“As an educator, we are trained that if you want to be effective, you have to know how to speak to your audience. As a CISO, I have multiple audiences, and I need to speak to each of them in language they can understand, that resonates with them – same as I do with my students,” said Smiley, the chief information security officer at Serco, a contractor for the provision of government services.

“When I’m speaking to the board of directors, I’m speaking with the language of liability,” he said. “With operational executives, you tend to have conversations about the bottom line and how to achieve our mission with a reasonable risk tolerance. With legal, the center of most of our conversations is material impact – explaining to them that we won’t be eligible for a $15 billion pipeline if we don’t get externally certified as being compliant with our customer’s requirements.

Longtime academic

Smiley’s professional experience has ranged across a wide variety of areas, including technology-related roles and operations management. He’s held just as many educational positions, doing things like curriculum development, writing books, creating training modules, developing courses and training.

He’s been in academia for 22 years, and as adjunct dissertation chair at National University in Arizona, is helping doctoral candidates get their PhDs, largely in business and technology.

His biggest challenge is something he shares with most CISOs, he said.

“Our mission is generally not very well aligned with where we are organized on the org chart and where we report to,” Smiley said. “Very often, we are reporting to someone with a different mission – generally the CIO or CTO – and our messages are filtered, sometimes to mask inconvenient truths.”

“If we’re not in the room when decisions are being made, I don’t know how we can properly influence those decisions to be less risky while still allowing the organization to meet the mission,” he added. “We CISOs only have the ability to speak to who we’re allowed to speak to in the ways in which we’re allowed to speak to them. That might sound harsh, but it’s the truth. We’re still light years from where we need to be.”

Be shrewd

Because the understanding of the role and the mission of the CISO is not where it needs to be, a CISO needs to be shrewd, he cautioned.

“A lot of times we will be invited to personally take on liability and risks that no individual should ever be taking on with relation to cybersecurity protocols – especially in organizations that are not as mature,” he said, recalling how a defense contractor recently had to pay a $9 million settlement for misrepresenting its compliance with U.S. government security requirements.

“I tend to use colorful language and then say, ‘No.’ We have to be very, very, very shrewd.”

One thing Smiley and his staff are heavily focused on right now is automation.

“We’re trying to automate anything that is predictable and repeatable, and there’s quite a bit of that,” he said. “We’ve been chewing on it and we continue to chew on it and we will be doing so for years.”

Panel interviews

Another change they’ve introduced are panel interviews of would-be employees, where the candidate is scored in a variety of areas -- some technical, others not -- to try to get a quantitative sense of whether they would be a good fit for the team’s culture. And then the panel – basically run by the team’s leads – solicits feedback from the rest of the group.
“Since we started doing this two or three years ago, it has worked almost 100% of the time,” he said. “I’ve definitely seen the difference because now the people who are on the team pull the weight collectively. That was not the case years ago. I had superstars and I had marginals.”

Smiley has also been actively designating people with primary responsibilities and support responsibilities to help with coverage, and that has worked well, too, he said. “All these things together really helped to support the team culture,” he said.

Employers have to open their purse strings and invest more time in training people if the cybersecurity talent shortage is to ease, Smiley said.

“It costs money and time to get people up to standard where somebody else would want to poach them, and nobody wants to do the training and raise them up. Everybody wants to do the poaching,” he said.

Press in

“The other aspect of the workforce shortage is the overwhelming majority of employers that have open positions are being way too cheap,” he said. “The shortage wouldn’t be anywhere as big as it is if the problem makers would acknowledge what they’re doing.”

For those trying to get a job, “press in,” he advised.

“If you don’t have work experience yet, say you’re a student, there’s nothing stopping you from standing up your own lab, or getting familiar with tools by using trial licenses or freeware. There’s stuff out there on the internet where you can go and play in other people’s sandboxes at no cost, where you can expose yourself to tools that are commonly used.”

Other options are internships, involvement in groups that do “Capture the Flag” exercises, or getting certified, he said.

“That’s what I look for if you don’t have any work experience,” he said. “If you’re just going to school and have not made efforts beyond graduating, there’s always somebody who is making the effort and showing they want to be part of this field. So that’s who I consider. So wherever you have an opportunity to reduce your ignorance in the space, take it.”

Consolidating spend

With the cybersecurity landscape changing so quickly, a top trend Smiley sees is consolidation of technology spend.

Companies like Microsoft whose security technology was once considered a joke have invested heavily in improving their space in the security market, Smiley said. And it’s those companies that are getting serious about security and bundling technologies that are going to win the budget, he said.

“When you go to those who hold the purse strings, and especially for those organizations that aren’t currently where they need to be in their technology and security tool stacks, it’s huge to be able to say, if you get this license, you can get 20 things,” he said.

Companies like Microsoft and Cisco will continue to buy companies, and roll their technology into a bundled package, he said. “I’m actually able to get certain technologies in this environment that I wouldn’t have had a chance in hell to do before bundling and aggregating,” Smiley said.

Video gamer

As someone with a part-time job as adjunct faculty at a university, and a full-time job at Serco, Smiley doesn’t have much free time.

“With what little time that’s left over, right now, I predominantly take my kid to the water park that’s close by,” he said. “We have a wonderful water park here in this county, it’s got a lazy river and big slides and the whole thing. We go there almost every day.

“The other thing I do is play copious amounts of games on Xbox,” he added. “I like video games a lot. They’re quite mature nowadays from when I was a kid and it was Atari and Nintendo.”
Christine Vanderpool is the CTO and CISO for Florida Crystals, a multi-billion-dollar sugar manufacturer, but like many in the security community, her role has expanded to include so much more. Her duties today include everything from security and innovation to enterprise architecture, IT supplier management, communications, data privacy and zero-based budgeting, among other things.

While Vanderpool jokes the company’s leadership gave her these additional jobs to “stop her from getting bored,” they’ve also served as a way to understand better the depth of the organization she has been tasked to keep secure.

“Too often as CISOs we focus on the traditional security roles of our job and do not take the time to understand the whole organization,” Vanderpool said. “I’ve been able to really understand the processes in our company, the supply chain, finance, legal challenges, and the ‘crown jewels’ that may be at higher risk.”

Vanderpool joined Florida Crystals in a traditional CISO role, following more than a decade at Molson Coors, expanding roles in information technology and security. As she’s grown in her career, her mission continues to expand beyond the CISO office and into part of a company’s larger leadership and technology team, along with that of a valued mentor.
Speedily changing technology

Vanderpool leans on an experienced team to fill in some of the gaps to take on these extra responsibilities. Her additional tasks allow her to expand her knowledge of Florida Crystals while empowering team members to take on more responsibility as she serves in a mentorship role.

Her current special project focuses on risk and business continuity planning for the company. While Florida Crystals excels at sugar manufacturing, the company features many different components from factories and real estate to an investment banking arm and an all-inclusive resort, among many other business interests.

“There are a lot of different areas that someone does not immediately see when they look at our company,” Vanderpool said.

“I want to look inside the core business and try to create a top-down strategy that looks at our security and risk profile to move the organization forward.”

Along with empowering others in her department, Vanderpool also makes an effort to understand the needs of each employee and ensure a cohesive working arrangement. By keeping employees happy and engaged, she ensures they continue to grow.

That structure allows for a highly functioning department that can expand beyond its traditional operating limits. Part of this mentorship, Vanderpool says, includes finding ways to keep work fun when possible. Years ago, she had the habit of ensuring every Friday meeting included a bad “dad joke” to keep everyone loose.

“I found out from a co-worker that when I left that company, they continued to make a bad joke of the week,” Vanderpool said. “I thought, ‘that’s pretty awesome. People remember that stuff.’
Understanding the Role of the CISO

One area Vanderpool tries to focus on, and she advises to those she mentors, is that CISOs need to understand the business case for security operations better. CISOs must tell a strong security story so their work is seen beyond just the backroom technology.

For instance, when she first started with Florida Crystals, some company leadership did not understand the full importance of information security. “There was this thought, ‘Oh, we make sugar, what information do we have that people want?’” Vanderpool said. “As a CISO, it was my job to get them to understand that things like customer information, banking data, and supply chain partnerships all offer security risks that we must plan for or we could end up with a real problem.”

As she continues to expand her roles, Vanderpool advises other CISOs to, of course, push for the security needs of their organization but also to see how they fit in the overall picture. She finds herself in an enviable position where the company leadership will approve security measures if she sees the business case. That doesn’t mean she goes full force on everything she immediately needs.

“It’s about getting past that single vision of security and how the full enterprise can be successful,” she said. “When we get beyond our scope, though, we can see how else the business can succeed. It’s about knowing when security is needed and when other parts of the organization may need those resources so you all can be more successful.”
JASON WITTY
USAA CSO
There's an extremely high degree of learning agility that every CISO needs, and a high volume of change that the CISO needs to anticipate and be aware of.

Jason Witty is a martial arts polymath. He has a 3rd degree black belt in Korean Hapkido. He does Japanese sword fighting. On weekends, he practices the Israeli self-defense and fighting system, Krav Maga.

That martial arts sideline has come in handy for his day job as CISO of the United Services Automobile Association, a Fortune 500 diversified financial services group of companies.

“People ask me if I’ve ever had to use it in my CISO world, and I tell them, I use that training every single day,” Witty said.

“It’s the discipline, the order, the ability to stay cool under pressure, the ability to know that an outcome is possible and know what tactics could and should be deployed for any given situation,” he added. “So yeah, I use it every day.”

Today, Witty’s No. 1 challenge as USAA’s top security chief is digesting, internalizing and institutionalizing the changes that are happening every day. And they’re myriad, whether it’s regulatory changes, compliance regime changes, emerging technologies and legal changes, or changes in the threat landscape, adversarial tactics or geopolitics, he said.

“I spend roughly two hours every morning just digesting what changed since I went to bed the evening before so that I know what I need to account for just that day,” he said. “There’s an extremely high degree of learning agility that every CISO needs, and a high volume of change that the CISO needs to anticipate and be aware of.”

As an example, there is a lot of hype now around quantum computing, so CISOs need to move off encryption algorithms that are not quantum resistant, Witty said.

“It takes a long time to move the internet off of vulnerable technology,” Witty said. “Up to 40% of the internet is still running old infrastructure. As CISOs, we have to start thinking about things that are not just right in front of us, but are three, five or 10 years out, because there are certainly risks that will take us a decade to manage.”
Witty started his career as a Unix systems administrator for NASA back in the early 1990s. Hackers were constantly breaking into the systems, so one day, he got onto ARPANET, typed in the word “hack” and found 1,300 documents. He printed those out, spent several years reading them while in college, and by the time he went back to NASA after graduation, he came on board as a Unix system security administrator.

“Security wasn’t a thing at the time, it was born more out of necessity, but that then launched into a number of other roles of increasing complexity over time,” he recalled.

These included a job as network security consultant at Allstate insurance, and various other security positions in financial services, including at Bank of America, U.S. Bank and JPMorgan Chase.

About a decade ago, he made the transition to reporting to the board. That’s when he realized that “there is a very massive difference between being able to speak publicly and being able to speak to a board.

“With public speaking, you want to be good at storytelling,” he said. “In a boardroom, you are there for corporate governance reasons. You have to transparently present risks and action plans associated with lowering those risks to ensure that you are adequately performing your fiduciary responsibilities as CISO.”

The Securities and Exchange Commission is currently formulating policy on how to ensure public company boards understand how security issues translate to an organization’s operational risk. In the interest of corporate governance, Witty personally prefers that every board director receive regular education on cybersecurity, rather than have just one expert – a CISO – on the board.

“If there is a CISO on every public board, then from a corporate governance standpoint, everybody is going to look to that person as the cyber person, and depend on one person who has a singular view on a particular topic,” he said.

“The approach we’ve taken on the boards I’ve reported to is make sure that there’s a fairly robust training schedule or set of training-related presentations for the board that explains the threat landscape, the risks, how technology changes that, and why we have to make decisions so quickly in the cyber sphere,” he said. “If the board is educated enough, they could credibly challenge management in a much more diverse way than if you just have one expert.”

He expects things will go in both directions. “I think you’re going to see CISOs joining boards as the expert, and I think you will also see CISOs suggesting the whole board get more educated on cybersecurity,” he said.
Since Witty entered the financial services industry in 1997, “the role of the CISO has changed quite a lot,” he said.

During the 20 years he was in Chicago, he ran an email distribution and dinner group for CISOs based there, giving him an opportunity to observe CISOs at a very practical and frequent level. By the mid-2000s, he was shocked to discover how so many people could hold the same title, but do such completely different jobs.

Today, while there’s still variability from industry to industry, he sees a lesser degree of variability overall than he did back in 2005, when CISOs were only responsible for setting security policy and had no operational responsibility at all. There’s a corollary with the evolution of the CIO’s role to becoming a business partner who helps with the bottom line and makes things more efficient, automated and digital, he said.

“The CISO is actually going through a very similar transition, needing to be somewhat technical and understand technological nuances, but at the same time, being able to translate whatever risks you’re managing in a truly risk-based language to the board or to the CEO or to the CEO’s direct reports,” he said.

“You have to really be a partnership-oriented person with a high degree of learning agility and a good executive presence within the board,” he added.

“But at the same time, you have to be able to manage risk well and grow a team, and build leaders who are going to build other leaders, and keep track of the ever-changing threat and technology environments.”
CISOS CONNECT™ PARTNERS

BLACK KITE

FORTE GROUP

Mayfield

Qnary™

uptycs
Secure cloud, containers, and endpoints with one unified solution.

Find and remove critical risks in your modern attack surface—from laptops to containers—all from a single UI and data model.

Shift up your cybersecurity

Visit uptycs.com

AUTOMATED THIRD-PARTY RISK INTELLIGENCE

Get your free Ransomware Susceptibility Report:

WWW.BLACKKITE.COM