CISO SPOTLIGHT EDITION

CISOs CONNECT™ MAGAZINE

FEBRUARY 2024

INTRODUCTION

AMY TEIBEL
VP OF CONTENT, CISOS CONNECT™

It is with great pleasure that we release the second Spotlight edition of CISOs Connect Magazine, highlighting the accomplishments and lives of chief information security officers on the front lines of the war against cybercrime.

Many of the industry professionals who appear in this issue are recipients of CISOs Connect's Top 100 CISO (C100) awards, a leading industry recognition honoring pre-eminent security leaders across the globe. And that's no coincidence: It is one of our top missions at CISOs Connect to celebrate those security leaders who are in the vanguard of protecting sensitive data and information from malicious actors whose sophistication grows with each passing day.

Because being a CISO is such a demanding role, we also want to showcase the individuals behind the technological and business leadership they represent. These are our professional peers, but they are also men and women whose drive manifests itself in exciting hobbies like skydiving, and meaningful after-hours contributions to humanity through projects such as financing microbusinesses in Africa.

Additionally, this edition seeks to highlight those CISOs who are now channeling the vast experience they've acquired into other, related ventures benefiting the cybersecurity community and society at large. Seeking new and different experiences, they have branched out into venture investing, consulting and working with vendors. Some have used the CISO position as a stepping stone to other executive roles, such as chief information officer. Being an organizational CISO need not be a final stop, and this journey is one that deserves our attention.

The exceptional group of leaders who appear in this issue play critical roles in global cybersecurity. They are truly an inspiration, and we hope you enjoy learning more about them.

Amy Teibel

IN THIS ISSUE

ON THE COVER SHAWN BOWEN. READ MORE ON PAGE 4 . PHOTO PROVIDED BY SHAWN BOWEN.

SHAWN BOWEN

WORLD KINECT CORPORATION CISO

Somersaulting out of planes at 14,000 feet with his wife is how Shawn Bowen escapes the pressures that come with being a CISO.

"Life is all about managing risk, and adequately preparing for that risk so that you can get the most reward out of it," quipped Bowen, the Chief Information Security Officer of World Kinect Corporation, a Florida-based energy, commodities, and services company. "It's all about getting to do bigger, better, new things. But the enjoyment that it generates means balancing this risk of the downside."

Bowen's professional life started at age 17 when he joined the U.S. Air Force Reserve, where he served nearly 25 years in the cyber warfare domain. On a parallel track, the self-educated technologist worked as a mainframe operator; did quality assurance on code and development; carried out various engineering and architecture roles; led security programs within IT functions for the Department of the Army; became the first CISO for Marine Corps Intelligence; and ran the cybersecurity program at one of the big U.S. intelligence agencies.

His career took a sharp swerve when he left the structure and foundation of government work to join what he referred to as a 180° opposite of that -- the world of franchise restaurants as the first CISO of Restaurant Brands International, the parent company of Burger King and Popeyes. Two and a half years ago, he joined World Kinect.

While single, he traveled down a third, simultaneous track, too.

"After work, I filled my time with everything that was interesting to me: playing sports to the highest level I could accommodate, being 'shipwrecked' for 10 weeks on a Pacific island for a reality TV show, and dabbling in other career fields for the experience and perspective. I was a volunteer firefighter for over 7 years, spending as many hours at the station as I was in the office. People like to use analogies of cybersecurity being like firefighting. Well, I've done that," he said, pointing to his fire helmet in the background. "They also compare risk to jumping out of a plane. I can tell you about that, too!"

These various threads, Bowen says, kept him grounded.

"While I was a CISO making decisions for the Marine Corps Intelligence enterprise, I was just the firefighter on an engine, with people above me. That gave me a good awareness of the realities at that level of how people are thinking and operating. Sometimes, when you only sit in your office or boardroom, you lose touch with how people are really doing things."

Bowen's biggest challenge at World Kinect Corporation is the company's multiple mission sets. Its diverse offering includes supply, logistics, sustainability, price risk, transaction management services, aviation support, flight management applications, private airport management technologies, rewards programs, air chartering, and government solutions around land, maritime, aviation and renewable energy.

"The breadth of our offerings changes my risk profile throughout," he said. "I have different brands or products with completely different profiles. Trying to build those discreet risk profiles based off of the impact that a threat exploitation could have can vary vastly from one profile to the other."

Bowen gets to bring a lot of security innovations into the organization. This summer, the business migrated all 22 of its worldwide data centers to the cloud. It's already replaced all its telephony-based call centers with communications via video conferencing.

By getting rid of on-premises networking where possible and going to SD-WAN, the organization has achieved greater diversity and a competitive edge, "where we're able to quickly modify and migrate some of our offerings as customers' security demands grow," he said.

Because the business is low margin, his team seeks to do more with open source and automation and uses technologies like ChatGPT to streamline some of its work.

“With the number of vendors solving every possible problem in cybersecurity, too often people look for a new tool to solve the problem. We’re constantly challenging each other to find new ways to use our existing tools that maximize that value, or simply building it ourselves,” Bowen said.

Participants in the company’s internship and new graduate program are constantly being challenged to bring things in with what Bowen calls a “college budget.”

“Living on ramen and mac and cheese? Apply that to our technology stack where possible,” he said. “When you’re limited in what is given to you, you tend to think outside the box.”

In that vein, his team no longer applies the same risk profile to every part of the company.

“We tailor threat modeling based off of the individual risk profile,” Bowen said. “That’s one of the many things that we’re trying to change in the way we approach things here so that we are spending the right number of resources protecting our enterprise.”

For new entrants to the field, Bowen advises learning the technology first.

“There are a lot of people coming into cybersecurity who need to write a policy or partner up with IT to secure an operating system, and they’ve never managed the technology, so we’re inflicting pain on our IT peers,” he said. “It’s critical to take that time to gain experience on the IT side.”

He also advises newcomers to practice threat modeling all the time – and not only on cybersecurity.

“If I’m going on a five-hour road trip, what's the likelihood of a flat tire? Where are my charging stations? Do I have kids in my car that need entertaining? The more you actively practice that threat modeling habit and critical thinking, the more natural it becomes and the quicker you can respond to cybersecurity threats in time of need.”

As the CISO’s role evolves, Bowen sees the industry headed toward greater differentiation. While there is commonality within the CISO community, different types of requirements are needed for different types of industries, he said.

"With the SEC's recent ruling on cybersecurity ensuring Board oversight of threat risks and management's role in assessing and managing those risks, it will become increasingly apparent that not all CISOs are experienced to discuss cyber risk in the language of the business. But it also shows that the language of the business is evolving to include cybersecurity, and that will highlight the number of executives that don't have the same understanding of cybersecurity that they possess about other critical segments to run a business such as legal, finance, people skills, etc.," he said. "It is our responsibility to better ourselves as business partners, and it is our opportunity to educate our peers on the cybersecurity impacts in a way they understand and care."

"A lot of CISOs are locking arms and saying, 'Hey, we're CISOs and here's what we need as an industry,'" Bowen said. "But as we've made that headway, we now need to start talking about the different requirements. You don't necessarily want a cybersecurity or CISO-certified person of a software company on the board of a manufacturing company."

As more technology becomes accessible to more people, the more complex an organization's security posture will become, he said.

"Ordinary people are using artificial intelligence and other technologies without understanding the gigantic iceberg below it," he said. "Threats have always been infinite, but now they're more accessible. That changes how we respond and build a defense program."

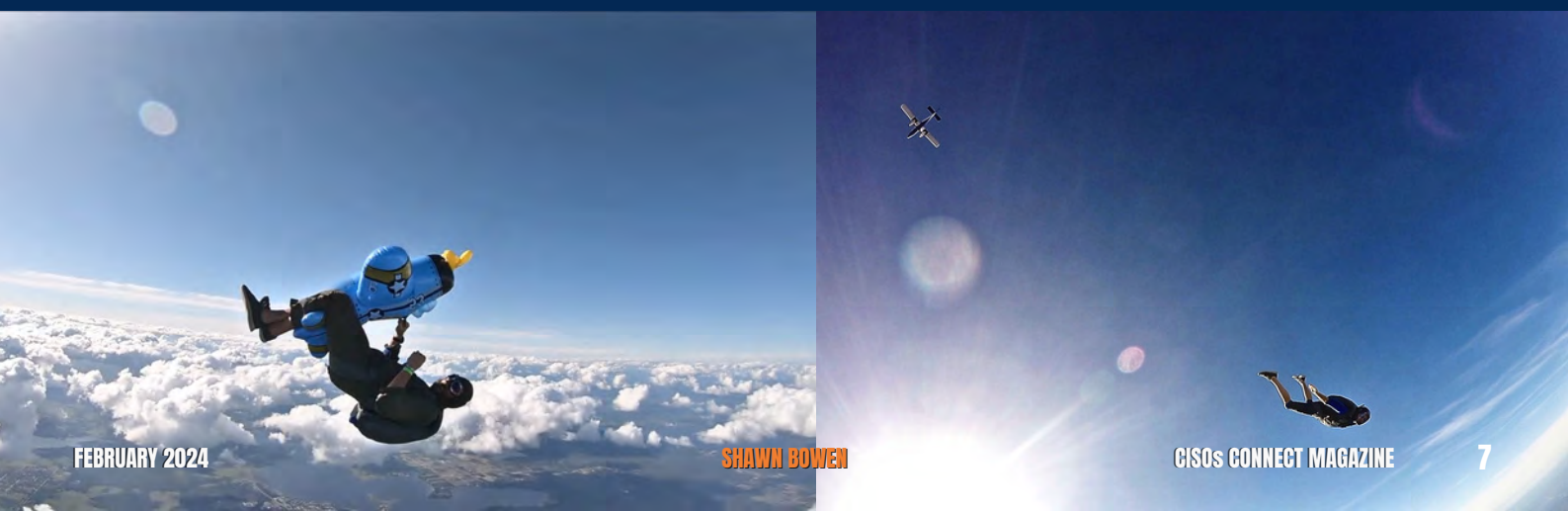
"A successful CISO will know how to talk about that iceberg in relatable terms to business leaders so they can understand both the risks and the threats, and the value CISOs bring to the business and its bottom line."

Bowen would like to see the codification of best practices that organizations should follow to protect corporate and customer information.

"Even a standard slide that every board member needs to see would be something that I think would simplify," he said. "We say we want standardization, yet we immediately argue over what the standard should be."

When Bowen was a teenager, his father told him, "Don't ever say you want to do something, say you did something," and that's been his guiding principle. Things like firefighting and being shipwrecked have given way to an amazing wife and two young children who keep him busy and put the smile on his face, but video games and skydiving complement the work he has a passion for.

"The games are how I stay in contact with my family," he said. "Skydiving gives me a little bit of adventure and mental distraction. If I'm thinking about anything other than that, I'm thinking about the wrong thing, because landing in one piece is the highest priority."



MONTAE BROCKETT

DISTRICT OF COLUMBIA'S HEALTH CARE FINANCE CISO

Many CISOs eagerly turn to hobbies to ease the pressures that come with the job. Not Montae Brockett.

"For me, unwinding is cybersecurity," said Brockett, the Deputy Chief Information Officer and Chief Information Security Officer for the District of Columbia's Health Care Finance agency in Washington, DC.

"My colleague said to me the other day, 'This isn't work for you, is it?' And I said no, because I love it. I eat, sleep technology every single day. It's a rare night that I don't pick up a cybersecurity book. I read constantly. I'm on my computer every night until 3 o'clock in the morning studying or training. And that's because I have a goal in mind, and I'm always reminding myself that I'm not where I want to be."

And where does he want to be?

"I want to be one of the top technologists in the United States and eventually the world," Brockett said. "My dream is to establish a cyber security company, which I have started, and for it to be successful. And to be able to employ individuals from my community and communities that are underserved in the cybersecurity space."

His company, Cyber Defense 3, is a boutique, woman-owned consulting firm focusing on risk reduction, compliance, governance and establishing information security programs. The goal within the next two to three years is to move into the defense and intelligence space and provide services to organizations that are on the front line defending the U.S. from threat actors, he said.

Brockett didn't start out in cybersecurity or anything remotely related: His bachelor's degree is in accounting. But he was bitten by the bug as a senior in college and has not looked back since.

He started out as an information system security engineer at an academic consortium, and for the past 15 years, has been working in the public sector. During more than a decade at the DC Department of Human Services, he matriculated from security engineer to CISO for the department's human services programs, including cash and food assistance, overseeing cybersecurity for the entire agency.

Humility, Brockett said, is the most important trait a CISO can possess. "We have the stigma of being unapproachable," he said. "Having that sense of humility allows you to engage others more, try to be more collaborative."

He's been in his current role at the DC Department of Health Care Finance for the past year.

"Being able to be in the weeds of technology innovation, understanding the program side of it, positioned me to be able to have success in an environment that's complex in its regulations, its governance, and the importance of the services that they are delivering," he said.

Brockett identifies three main challenges to his job: balancing customers against risk exposure for the agency; modernizing the environment; and getting buy-in for new initiatives that could have an impact on the delivery of service to customers.

The biggest innovation he is trying to introduce is leveraging technology to replace some of the manual processes in place, "to make our jobs more effective and efficient as we deliver services," he said. "Supporting the adoption of cloud technologies will be key to positioning us with new technology and putting us in a continuous stage of innovation."

It's time for CISOs to stop leaning on the "users are the weakest link in the supply chain" argument, Brockett said.

"We can't blame it on the users because we understand the environment," he said. "We should account for the known and unknown to prevent or mitigate risk to an organization or that user.

"Our perspective has to be understanding the business operations and business process, and collaborating more effectively across the environment," he said. "Organizational divisions often work in silos, and that actually reduces your collaborative efforts, your efficiency, and your effectiveness to deliver a successful project for your user community."

To reduce these obstacles to collaboration, Brockett favors informal meetings to discuss creative ideas in an open format where people can comfortably communicate.

"We're not sitting at a table with our pens and pads waiting for direction to drive the conversation," he said. "We're creating an environment where we all can just facilitate ideas. It's the first step in having buy-in from your stakeholders and users of a specific project. We need to let ideas sprinkle through the entire ecosystem, because it's through inclusion that we improve."

Humility, Brockett said, is the most important trait a CISO can possess.

"We have the stigma of being unapproachable," he said. "Having that sense of humility allows you to engage others more, try to be more collaborative."

At the same time, being authoritative is also imperative because CISOs can be faced with decisions that go against their principles as security officials, he added.

"We have to be able to articulate and provide communication to senior leadership, provide the context they need with regard to requests they make," he said.

Brockett expects to see more CISOs sitting on boards and in the C-suite "to be able to provide context on where the organization is from a risk and security management standpoint," he said.

"Those are the things that are going to be the nuances of this role, that you will be required to be able to provide that performance-based evaluation to senior leadership so they can make decisions."

For those entering the field, the most important thing is to take advantage of all the resources available for security practitioners, Brockett said.

"Don't wait on anyone to provide you with the resources that you need to do what you want to do," he said. "There is so much free training that can educate you in the various technologies that are being used throughout a lot of organizations and environments," he said.

"I read every single day. I buy books, I buy training platforms, and when new technologies come out I immerse myself in them. There is so much material and so many opportunities out there, including social media platforms where you can communicate with people who can drive you in the right direction."

There are so many unfilled jobs in cybersecurity because individuals aren't educating themselves in the new technologies and getting the skill sets that organizations need, said Brockett, who is developing a training platform for at-risk youth interested in entering technology.

"Have you ever built your own lab? When you get into interviews and they ask, 'Why should I want you?,' if you have practical knowledge and actually built these things, then even without experience you've demonstrated that you can build all of these technology solutions yourself," he said.

"You have to challenge yourself and show that you have the drive to learn. That's one of the biggest traits that you have to have getting into the cybersecurity profession."

DENEEN DEFIORE

UNITED AIRLINES CISO

Deneen DeFiore was completing a master's program in healthcare administration when she stumbled into technology and cybersecurity.

"We were switching to electronic medical records and I kind of just gravitated to that, understanding the process and connecting all the dots. So I ended up moving into the technology space, and then evolving over time," recalled DeFiore, Vice President and Chief Information Security Officer at United Airlines.

After taking on various roles in infrastructure technology, she went to work as a Chief Information Officer for a small business unit, where she experienced her first cyber incident. She learned quickly and tackled it on the fly, because such incidents were rarer in those days.

"It just clicked with me: This is going to be the next big thing because at the time, every company was beginning to go through a digital transformation, and technology was accelerating different capabilities across different industries," she said. "I got through that experience and I was hooked."

DeFiore's career history set the theme for her career progression: Identifying a messy problem and figuring out how to fix it. She calls it "a journey with no destination."

"Every day is different. There are new opportunities, new capabilities, and things change on a dime," she said. "That has influenced how I determine what to work on, where I go next, and what I want to accomplish."

At United, DeFiore manages cybersecurity and digital risk across an aviation ecosystem that ranges from network protection to connected aircraft. She joined the airline six weeks before the Covid-19 pandemic struck and had to pivot into crisis management almost immediately.

"We instrumented and secured remote access in a couple of weeks," she recalled. "What would have taken 18 months before took only a matter of weeks."

The move to United "was a big life decision," she said, taken after she had spent 19 years at GE, including six at GE Aviation.

"I was excited about taking on a new challenge and opportunity, but I had grown up in the company I was with previously," she said. "I knew the structures, the processes, the people, the culture. I had credibility going into United because I worked in the aviation sector, but I didn't have those trusted relationships. So for the first three months, even when managing a crisis, I was actively listening and understanding what people cared about and developing those trusted relationships. I'm not going to lie, there were days when I asked myself, 'What did I do?' But it definitely made me stronger and I learned at an accelerated pace. It was a great choice."

DeFiore's biggest challenge is connectedness and the scope of what CISOs have to think about. "We're managing systemic digital risk, but we've also to think about the broader environment we operate in," she said.

Another challenge is the pace of change in technology adoption.

"The way technology is consumed is a lot different than a few years ago," she said. "We have to create a framework so people can understand digital risk and the consequences of the choices they make. We're not always going to be embedded in every single project or every single initiative or conversation at the airlines, so we have to figure out how to make sure people have the right information to do their jobs compliantly and securely."

DeFiore sees a lot of opportunity to think about cybersecurity differently. When it comes to security awareness, for example, it's going beyond giving people information about how to detect a phish or suspicious email. "It's about giving people bits of information in the moment when they're doing their jobs, so they can recognize a risk and understand the consequences," she said.

She's also trying to do a lot of engineering solutioning to help United stay ahead of threat.

"We take advantage of commercial tools and platforms, and try to leverage them as much as we can," she said. "We understand the threat actors and the risks in our environments, and evaluate our commercial tools to figure out the gaps."

Like other CISOs, DeFiore is grappling with a personnel shortage, so she's looking at different pools of talent and transferable skills to get people into cyber. She's partnering with colleges for curriculum influence, and recruiting early on. She's also taking mid-career workers who didn't go the traditional college degree route and transitioning them into cyber.

With as massive an operation as United Airlines, you can't put controls in every part, DeFiore said. "We try to figure out where we can leverage the workforce to do their jobs, or raise awareness of opportunities for improvement, and work with our team to close the loop," she said.

United's cyber organization rests on three pillars.

"One is to be brilliant at the basics," she said. "Yes, we're doing vulnerability management, but we're also figuring out how to identify vulnerabilities quicker and remediate them faster, to make sure that baseline cyber hygiene controls are in place and continuously monitored so they are effective."

The second pillar is advancing the organization's capabilities as the threat and technology environments change. "We have to continuously look at our program to see what else we need to have to protect critical applications and systems and recover quickly," she said.



The final pillar is aligning to business goals and growth targets, as the airline acquires new aircraft, new hires, new terminals and new routes. "We need to make sure that we are designing securely and supporting those outcomes in a secure fashion," she said.

DeFiore has watched the CISO's role evolve from a technology-focused world to more of a business risk role.

"There has definitely been an accelerated shift in the past couple of years because of the threat environment that you see," she said. "Geopolitical conflicts are a much more tangible connection that business leaders are making, giving CISOs a role in risk-management discussions."

On a macro level, the volume of cyber attacks is rising exponentially, DeFiore said. "It's not just cyber crime, but even nation-states have shifted tactics," she said.

"We're not just looking at IP theft to gain economic advantage, but at a lot more disruption and disinformation as everyone moves into more digital interaction. There is a whole shadow industry that's fraudulent, like bogus travel agencies that claim to help you but take your money or your miles. Or illegitimate contact centers that are set up to scam customers. We've seen a real high spike in that. Digital fraud has been around forever, but it's more prevalent and in your face now."

A successful CISO, she said, needs a baseline understanding of technical concepts because most of the controls and approaches they put in place are technical. But business acumen is crucial, she added.

"You really need to understand what your organization is trying to accomplish and how you enable those outcomes in a manner that has a risk-management focus," she said. "There are tons of things that I, as a cybersecurity professional, would never do. But I understand the opportunity from the perspective of revenue generation or customer experience, so I have to figure out how to do it in a manner that reduces risk to an acceptable level."

As a rare woman in the CISO's seat, DeFiore urges women cybersecurity practitioners to have more confidence in their skills.

"One thing that I've noticed as a trend as a woman in cybersecurity – and this has been proven in a lot of research – is that we feel we have to have all the boxes checked to go after a job, instead of looking at what transferable skills we have, like baseline analytical skills and willingness and ability to learn," she said.

"My experience has been that despite ups and downs, when I have put myself out there, things have always worked out. I'm passionate about the industry. I like to learn, I like to do research, talk to people and connect the dots. I would encourage other women to think about that as well."

DeFiore does a lot of mentoring, and she also thinks sponsorship is important. "Having someone in your network who will sponsor and advocate for you – and even look out for you and push you into opportunities – is so important. I've tried to make it a priority to not only mentor, but where I can, have a trusted relationship, advocating for people, and women especially."

To relieve the relentless pressures of her job, DeFiore schedules time for herself. "I block out my calendar for three hours on a Friday afternoon so I can just level set, rest and think about what I need to focus on," she said. "I also work for an airline, so I'm going to take advantage of that and purposely take a week off every quarter to disconnect and be with my family. It's important to let your mind go, trust your team, and trust your operations."

Running allows her to clear her mind, and she also enjoys gardening.

Sometimes during repetitive tasks like deadheading perennials for two hours, "you get a great idea because you're not thinking directly about what's happening," she said.

"That also helps me to level set and get me a little grounded."

CASSIO GOLDSCHMIDT

SERVICETITAN CISO

For Cassio Goldschmidt, cybersecurity is an arms race, trying to stay one step ahead of the enemy. That's why building alliances is so important.

"I think the only way to really succeed as a CISO is to create allies," said Goldschmidt, the Chief Information Security Officer at ServiceTitan, a cloud-based platform that helps home services companies streamline operations and improve customer service.

"It's a matter of talking to the people you work with, and arming them with the tools to actually be able to detect malicious activities or anything that could get in their way," he said. "It's getting them to understand what the crown jewels are, what needs to be protected, what is public information, and bringing everyone to the battle. Not only your staff, but employees, vendors, partners and even customers."

Goldschmidt has been fascinated with software since his early teens, and started his professional career developing enterprise software for Fortune 500 companies. He began working with the security community 16 years ago, doing both product and program-level security.

"I've always been in high tech companies. Software is what they sell, and security is paramount because it touches their reputation," he said. "So having been the one actually developing code and being in the trenches really creates a lot of empathy and understanding of what it really takes in order to develop good software, and security plays an intrinsic part."

He was working at Symantec as a software engineer when he was nominated to become security lead for the group that was developing anti-virus software. With a master's degree in software engineering bolstered by an MBA, he was soon leading the product security group.

From Symantec, he went on to Intuit Financial Services, which was one of the first companies with financial data to move to AWS, and then served as vice president of the cyber resilience practice at Aon, a forensics company.

A successful CISO must be a technical person but above all a business person, Goldschmidt said.

"Constantly communicating with the business is paramount," he said. He meets frequently with customer success and legal because he sees his role as a business facilitator and not an obstacle.

"A lot of times, security is the Department of No, which stops things from moving forward," he said. "But you have to really work with other teams and make sure that you can go as fast and securely as possible. The CISO has to understand that this is not a game of liability. Let me work together with various different teams in order to achieve what needs to be achieved and be as proactive as possible."

Because every CISO has limited resources, it's important to invest in partnering with other companies and to know where to invest resources, "because there are some great companies out there," he said.

“CISOs really need to be one step ahead if they really want to be effective and provide value to the business,” Goldschmidt said. “Challenges vary by industry, but in my case, I really think the technology and the regulations are the real challenge.”

Goldschmidt meets with vendors several times a week to both understand what they’re doing and to influence their products so they can actually fit his company’s needs, he said. He sees that kind of collaboration with vendors expanding industrywide, especially in tight financial times when CISOs are looking to optimize solutions they already have.

“We’re working with our vendors to see what else we might have overlooked in the set of things that we already purchased that can help us,” he said.

Working closely with vendors is also critical to maintaining customer trust in an age when companies use a lot of SaaS and other software CISOs can’t control. For one small vendor, he not only wrote the security agreement, but also helped to find their first security hire, he said. “This partnership is more important than ever,” he said.

Keeping up with the rapidly changing security landscape is his biggest challenge.

“CISOs really need to be one step ahead if they really want to be effective and provide value to the business,” Goldschmidt said. “Challenges vary by industry, but in my case, I really think the technology and the regulations are the real challenge.”

“We’re living in unprecedented times,” he added.

“Everyone knows what AI can do, and that includes not only the good guys, but particularly the bad guys. And everyone is turning to security and asking, how should we use this technology? What is good, what is possible and what’s prohibited? You need to understand the technology really well, and at the same time, be able to provide insightful comments to people who are potentially ahead of you in the use of these things.”

In a “very, very short period of time,” he predicted, the solutions CISOs have relied on for years won’t be effective anymore because malicious actors will also be leveraging AI, he said.

“Business email compromise, for example, is going to be very different,” he said. “Once an account is compromised, AI will pick up from the last email the victim sent, continuing the conversation using the same writing style as the person who was victimized, building confidence through multiple emails before making a malicious request. And there won’t be any way for current software to actually detect this because it is a trusted email with multiple messages and so on.”

Because it will take time for tools to catch up, educating employees in security will be more crucial than ever and very challenging because people will also be writing messages like computers as they leverage AI, he said.

"We have to get this information in digestible forms continually to people, and in a meaningful way so they don't skip it," he said.

ServiceTitan has augmented its annual security awareness training with its Phish a Phriend contest, which invites employees to write their own phishing emails based on public information about the company available on the internet. The infosec department then sends out these employee-generated phishing messages to employees throughout the organization. By creating the phishing messages themselves, employees learn more about the concept of phishing, how it's done and how to detect it.

Another big challenge for today's CISO are the ever-changing laws around privacy issues, especially in the absence of unified legislation.

"Today, the CISO really needs to have a deep understanding of privacy. They have to create a trusted brand," he said. "A lot of companies are creating the position of chief trust officer, and that is something CISOs have to do these days. They have to talk to customers to make them feel comfortable and confident not only about the security mechanisms in the software, but also how their data is safeguarded."

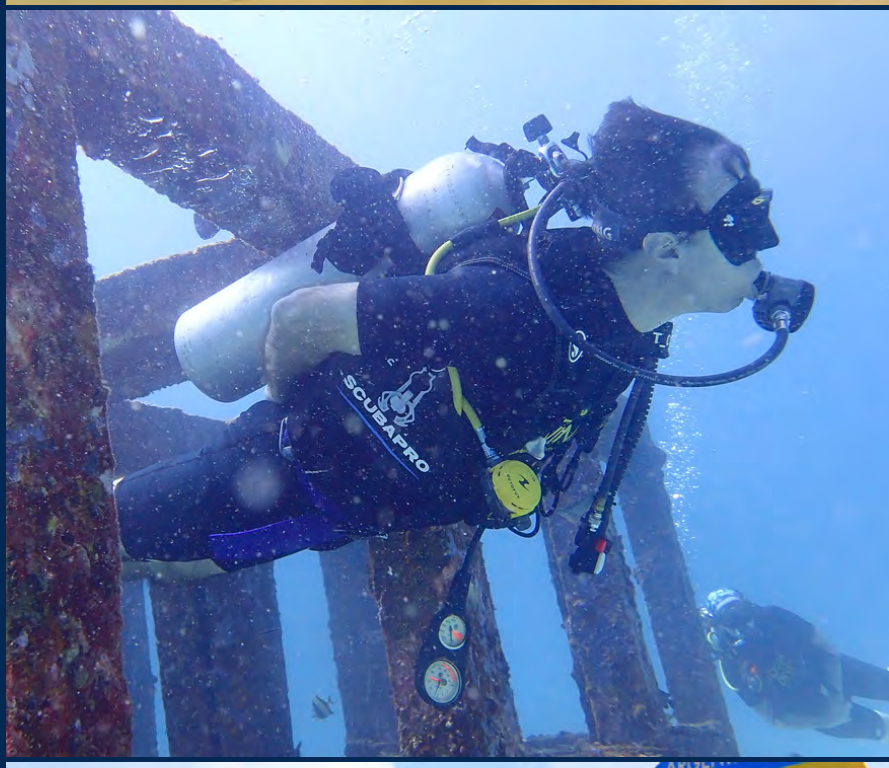
Goldschmidt is a long-time contributor to the security community. He has worked closely with open web applications, holding multiple positions at OWASP and co-authoring white papers for SAFECode.org. He has also volunteered for ISC2, advised VC firms and startups, and served on the CISOs Connect C100 Distinguished CISO Board of Judges since 2021.

"I think whatever time I put into the community I got back in the sense of learning from others, sharing experience and getting experience from others," he said. "I am very thankful for all this time that I spent and continue to spend with various communities."

When Goldschmidt has time, "I still like to get my hands dirty and do some software just for fun to understand the technology," he said. He also composes electronic music, "which tends to confuse my wife, who's thinking that I'm still working when I'm just having fun," he quipped.

He also makes family videos, and has won awards in international competitions, including for his film of a family trip to Yosemite using a 360 camera.

"Other places, you usually point a camera one way, because the other way is not as pleasant," he said. "But when you go to a blessed place like Yosemite, there's some places there that are just really beautiful all around."



BIL HARMER

CRAFT VENTURES CISO

Bil Harmer, Operating Partner, Security and Chief Information Security Officer for Craft Ventures, would love to see the CISO role go away.

"That means you've reached a point where you're all doing the right things," said Harmer, whose career has taken him to industries as varied as startups, a financial institution and even porn sites.

"We walk around telling people, don't walk down that alley, don't talk to that sketchy person. But most people know not to go down the alley at 2 o'clock in the morning. Today, 25 years and two generations of workforce into the commercialization of the internet, younger people are much more aware. They know what not to do. So I would like to see the CISO role transform into a risk role, where you're helping the company set the risk. "

Boards don't want to hear CISOs talk about the number of attacks they averted, or the patches they put out or the servers they cover, he said.

"They want to know, what's the risk to the business," he said.

"If you understand how the business makes money, then you will understand what to secure. It's about looking at the areas of risk and how they total up to company risk – and to be able to articulate and implement programs that reduce risk to acceptable levels."

Harmer doesn't even like the term "CISO," because it implies a separation between the physical world and the data.

"If you don't control your physical world, you don't control your data," he said. "Ask any good hacker and they will tell you, give me physical access to something and I will own you sooner or later."

Harmer disagrees that users are the weakest link in a security program.

"That is not true. They're the easiest target, and they're the easiest target because they're not trained," he said. "So we need to remove those decisions from them.

"We need to be able to ingrain in them the basics so they make safe, unrisky decisions. And then we put the other pieces around. Just like cars, right? We put three-point seat belts in cars. We put airbags in cars. The safety stuff comes by default. The same with security. The other pieces become less risky because you've taken away some of the bigger, greater risks and you've limited the impact that they can do."

,

In the mid-1990s, Harmer – then working at Sony of Canada -- proposed the company build an internal website to collect information amassed each day for a major project, instead of printing out workbooks nightly.

"I'll never forget these words, and I thank my manager for saying them to me. 'Why do you want to screw around with that internet stuff? The internet's a fad, and it'll be gone next year,'" he recalled. "So I quit."

Harmer took the experience he had accumulated building networks and websites and doing a little bit of security to the porn industry.

"I joined a friend at a company whose primary funding was adult content," Harmer said. "We built the second-largest porn site in the world called Smutland. In 1997, I pushed more traffic to the internet than all of Bell Canada's home internet users. So we were at the forefront."

Because the porn industry is attacked so regularly, he started building firewalls and intrusion detection and incident response systems.

"I'm at a point in my career where truthfully, that job is a badge of honor," he said with a laugh. "I built some of the biggest websites, one of them still in operation today. We were doing G3 live video broadcasts because we had access to all of this technology back then. I have plans to write a book someday, and the title of one chapter or maybe the whole book will be 'Diary of a Smut Peddler' because I just love that title."

As a university student, Harmer wandered into computer work to pay the bills so he could pursue a career in special effects. A summer job at data centers changed his trajectory, but he channeled his love of special effects into a lifelong hobby of building things.

For Halloween this year, Harmer built a Freddy Krueger knifehand – a companion piece to one he built when he was 18 and still has. It was a memorable day four years ago when he met *Nightmare on Elm Street* star Robert Englund at a convention and had him sign the original.

"You need a secondary thing that is not what you do every day," he said. "So this became my hobby. I started building masks, props, costumes, replica guns from video games.

"I built a 49 international pickup truck, and a 23 Ford Rat Rod. I also built custom motorcycles. My last bike was in the Austin Handbuilt Show in 2022. I like to play ice hockey as well. I'm just dumb enough to be a goaltender. So I'm out on the ice two, three times a week with people ripping 80 mile- an-hour pucks at my head."

Harmer's security career has taken him to startups like DocSpace, SuccessFactors, Zscaler and SecureAuth; financial institutions like Manulife Financial; and now Craft.

DocSpace was acquired by Critical Path, which later became embroiled in a securities fraud scandal. But it was there that he was first exposed to the business side of companies as Critical Path set out to rebuild.

"It showed me that side of the business, how decisions get made, how you have to make decisions very quickly in some cases if you want to survive," he said.

While at SuccessFactors, later acquired by SAP, Harmer pioneered the use of the SAS70 coupled with ISO to create a trusted security audit methodology used by the SaaS industry until the introduction of SOC2.

Act of survival

A presentation he created at Zscaler, called "Change is simply an act of survival," articulated from a security standpoint why companies needed to change their architecture to be able to work from anywhere.

"I had no idea what I was talking about would end up being the pandemic," he said.

At Craft, Harmer provides vCISO services to portfolio companies, and also functions as Craft's CISO.

His highly varied career history has influenced his execution of the CISO role.

"That's given me an empathy and an understanding that you have to look at things from everybody else's perspective," he said. "It's taught me that change is an act of survival. You need to adapt to the situation you're in."

A lot of security people tend to focus on their expertise, he said. "Get out of your comfort zone and start learning things," he advised.

Future of internet

For Harmer, the missing piece in security is identity, because there's no way to verify who typed the password.

"To me, identity is still the future of the internet, especially with AI and its ability to impersonate video and voice," he said.

"We need a much more global, holistic approach to digital identity that bridges both personal and business. That's going to be a while, but we're starting to see inroads there."

Harmer also expects big changes to emanate from the convergence of more real-time monitoring and execution with advanced, hyper-fast AI decision making.

"When those two collide, I think we'll have some amazing things come out," he said.

RAFI KHAN

NEW JERSEY TRANSIT CISO

Rafi Khan sees his career as a series of crossroads for taking his professional path to new levels.

Three factors help him to balance these decision points, said Khan, the Chief Information Security Officer at New Jersey Transit.

"One is the will to push back on system security compromises, whether it's corporate pushback or political pushback or even market pushback," Khan said. "If it's going to compromise my company, the safety of my staff or the safety of my constituents, I will not budge – unless you assume that risk and put it in writing."

The second has been a willingness "to pivot from one industry and then dive to another." That flexibility has taken him from a longtime career in health care to e-commerce, and now public transit, where he's tasked with protecting critical infrastructure and all the other touchpoints related to travel.

The third item has been "building the right culture within your team." That includes upskilling talent, which is key when you have a very competitive recruitment environment, he said.

"We ensure that we provide them all the right tools so they are not confined to some older technology that may not be marketable 99% of the time. That way they understand we are not short-changing them and they will not be looking outwards," he said.

"There's also our culture of providing a better work-life balance, the culture of understanding that we have your back. If something happens, there's no blame game. There are always lessons to be learned that we can evolve from to the next level of challenges. It's been successful."

Khan got into cybersecurity after studying and practicing nuclear medicine technology, a discipline that required a very strong understanding of computer analysis. That experience grounded his understanding of where computer technologies would be going, sharpened his awareness of data privacy, and taught him the value of empathy.

"Execution of the CISO role requires a deep understanding of who will be impacted in today's cybersecurity space, because so many touchpoints will be affected," he said. "If you have a vendor who has a vulnerability, for instance, how do you manage that? The execution will be a fine line between, 'Hey, you folks are compromised,' and 'We will not compromise our systems by exposure to yours.' And that fine line is saying, 'We understand that we are on the same side. We want to help you.' Let's help each other." The same goes for colleagues. CISOs cannot work in a vacuum. Partnership is very, very important."

Alliances with federal agencies and law enforcement is also crucial in his current role, where in addition to ensuring safety for NJ Transit's ridership, staff, data and systems, Khan must look outward to see what threat intelligence he might be able to gain.

A successful CISO, Khan said, learns from colleagues and shares what he learns.

"They will share with us some threat intelligence and they may even glean something from us. It's a two-way street. It is very, very important that we work together," he said.

Khan's program rests on three foundations.

"We have to intelligently select and continuously improve on our cybersecurity tool chest. We can't have gaps in the program. We always have to be looking at different technologies, and that's where the partnership with vendors comes in. And you always have to optimize, optimize, optimize. If you don't optimize your infrastructure to prepare for the next attack, it'll be more difficult when it happens," he said.

Khan is busy integrating artificial intelligence and machine learning within his organization's tool chest.

"We want to include security orchestration, automation and response to support our security operations folks," he said. "The logs we receive are voluminous. It's not humanly possible for even a huge army of analysts to review the intrusion attempts."

His team is also adopting a zero trust security strategy, with a layered defense approach to support it.

It's challenging to build a test environment that's reflective of a diverse ridership base that's approaching a million riders a day on weekdays. Networking with other players in the space is essential as technologies and bad actors evolve, Khan said.

"My team does an incredible job. But sometimes it's almost impossible to anticipate all the potential different scenarios. That's why we work very closely with other transit systems and law enforcement, because together we all provide each other the best intel," he said.

"The pressure is always on. We must always adapt faster. We must always look at new tech innovations and whatever our customers might be demanding," he added. "We have to balance things to make sure we are not leaving any vulnerabilities with our cybersecurity approach. I cannot remove guardrails, even when there are tensions to open up everything."

Early on in the job, Khan met with different business units to identify their security pain points, recognizing that communication with other departments and executive leadership is critical.

"We have to partner with communications folks. We have to partner with legal. We have to partner with executive management. We also have to look what's in the offing and communicate that risk to leadership. All of that will happen only if I have built that relationship, if I've had lunch with them, or coffee, to break the ice," he said.

Threats that occupy him are business email compromise, and the very high quality compute power that malicious actors can now harness to crack passwords. Third-party vulnerabilities are another concern.

"We're looking at their SLAs, putting their feet to the fire on them, because if they are vulnerable and don't have strong cyber hygiene, then doing business with them might be a risk," he said.

A successful CISO, Khan said, learns from colleagues and shares what he learns.

"You need to have an open mind because there will be times when you are jaded by your experiences and think you know what you're dealing with, when you may not. Therefore you have to confer. CISOs cannot be successful by their own thinking alone. My approach is always to consult, consult, consult. It's going back to the crossroads. We are at a crossroads every day in making decisions on how to mitigate risk, or how to enable business without adding risks."

Khan's advice to people just entering the field is to show humility.

"If we are humble, we understand there's always another thing or two or three that we'll be learning in the future. So stay humble, but also stay hungry," he said. "You're never done learning in cybersecurity. And if you do stop growing and learning, you have to understand that you have to realign and put the train back on the rails and don't stagnate.

"Another thing I'd advise is be there. If you have to drive a five-hour round trip to meet up with a group of talented people for a two-hour dinner – and I've done that – then do that to build your network. Showing up, in my view, is 90% of success."

Khan finds an outlet from the intense pressure of his job by rebuilding vintage stereo amplifiers and working on his Mazdaspeed3 sports car. Rebuilding amplifiers definitely has very strong tie-ins to his job because it's all electrical, he said. Working on the car is a similar extension because "it's all about understanding checklists, understanding what you've missed, and understanding how you can improve," he said.

"I drive a Japanese speed rocket," he said. "I like to tune it. I drive a six-speed, and I put in a cold air intake so it can breathe better and run faster, and gain horsepower. I changed the suspension to go around corners better. It's good therapy for me. It's fun. It keeps your brain tuned as well as your car tuned."

DONNA ROSS

RADIAN GROUP INC CISO

Donna Ross, having completed a degree in economics, was working in one of the business lines at Prudential, but colleagues kept coming to her for help with technical issues. This steady stream of traffic didn't escape her boss.

"I had a great mentor and boss, and he sat me down and said, 'You really need to make a decision about which path you want to take. Do you want to take a business path or a technical path?' And you know, the technical stuff really excited me," said Ross, the Chief Information Security Officer at Radian Group, a Philadelphia-based mortgage insurance company.

"Ever since I can remember, I've been a tinkerer. As a child of five or six I would take apart my grandmother's radio and put it back together. So, I found a career that works with how I think. I didn't even know it until this boss of mine, this mentor of mine, explained, 'This is how you're wired. There's clearly something in this if people are coming to you.'"

Shortly after, a colleague who ran the security practice at Prudential asked her to work for him.

"I told him, my degree is in economics. I know nothing about security," she recalled. "And he said, 'It's OK. I see something in you.' And shortly thereafter he retired, and I got promoted. I found this passion that I have carried with me throughout my career."

"I'm a continuous learner, and security is a practice where you're constantly learning and adapting. Every day is different. You don't know what you're going to expect from one minute to the next. And that excites me," she said.

Ross is paying forward the life-changing mentorship she experienced.

"I work hard on coaching, mentoring and championing people," she said. "People are my greatest asset. When you think about security, there's people, process and technology. There are a lot of cool technologies out there. And for technology to work, you have to have processes. But the people are what make the material difference."

The top priority in her role is enabling business success by protecting the data the organization collects and uses, safeguarding the technologies it employs, and allowing the safe operation of applications.

Security, she said, is a team sport and should not be the company's best-kept secret.

"Security is everybody's job. It makes the program more accessible, builds confidence in the program, and results in more effective security," she said.

That team spirit must extend to collaboration and information sharing within the broader industry, she added. Her own affiliations with the security community include the CyberEd Board, Women in Cyber, ISACA and FS-ISAC.

After Prudential, Ross built the security practice at GMAC as it was opening its first bank, then replaced the retiring information protection officer at Corning. She joined Radian more than six years ago.

Ross calls herself a "builder CISO."

"I was the first CISO at Radian. I was the first security person at GMAC, and I was the first official titled person with a security background at Corning. They sent me to places where they don't have a program, and I got to build out the program, hire the staff, develop the policies, and improve the program," she said. "I want to do the hard work and build out the program and grow the talent. To me that's the most fun."

She also calls herself "a Diversity, Equity and Inclusion evangelist."

"All four of my grandparents were from Eastern Europe and I saw the hardship that my grandparents had when people would misinterpret an accent for ignorance. I became an empath, and as a result of that empathy, I became an advocate, and as I gained more influence at work, it became really important to me to use that power for good," she said.

Her background has led her to advocate for equal pay and visibility for women, coaching African American professionals, and sponsoring LGBTQ professionals, among other things.

Being a woman in tech is always challenging because it's a male-dominated field, but it's taught her a lot about timing, she said.

"What I learned to do, and it's unfortunate that women have to do this is, you speak at the right time when you have the right information, so that when you don't speak, your male boss will ask you, 'Donna, what do you think?'"

Another way to deal with the gender imbalance is to develop an expertise beyond your field, Ross said.

"When I have that seat at the table, when I sit on a staff, I should be able to speak to strategy, leadership, budgeting and employees so they don't look at me as Donna, the security person," she said. "They look at me as another leader who has a seat at the table and raises the right issues."

Ross has a degree in marketing, and that's made her "very, very customer focused," she said. And while technical skills are very important in security, it's the soft skills like communication skills, collaboration skills, project management skills and leadership skills that are the differential, she said.

"If you can't be in a room of executives and talk to them in plain English in a way that they understand, you're not going to be successful," she said. "We have a standing item on our leadership agenda: We meet once a week on elevator pitches because the person needs to be able to represent their program in 15 seconds."

Doing differential work is what distinguishes her team and makes it so valuable to the company, she said.

"My team does not turn cranks or watch flashing red lights or green lights. Managed service providers do that. Where we add the value is helping our business grow."

By outsourcing the commodity work, she also frees her team to do "fun stuff" like threat hunts and purple teaming when they're not serving customers, or to take training classes to learn about new developments in the industry, she said.

"I think the culture of getting away from commodities and shifting to what's important to the business is really core to how I've built the programs," she said.

Adversaries are getting smarter, geopolitical events aren't going to slow down, and more groups are going to work together, Ross predicted. Supply chain security is another worry.

CISOs continue to get a bigger seat at the table as their role becomes more visible and they become an intricate part of the business, as business leaders as well as security experts. Liability and regulatory changes are a more troubling part of where the CISO's role is going, she said.

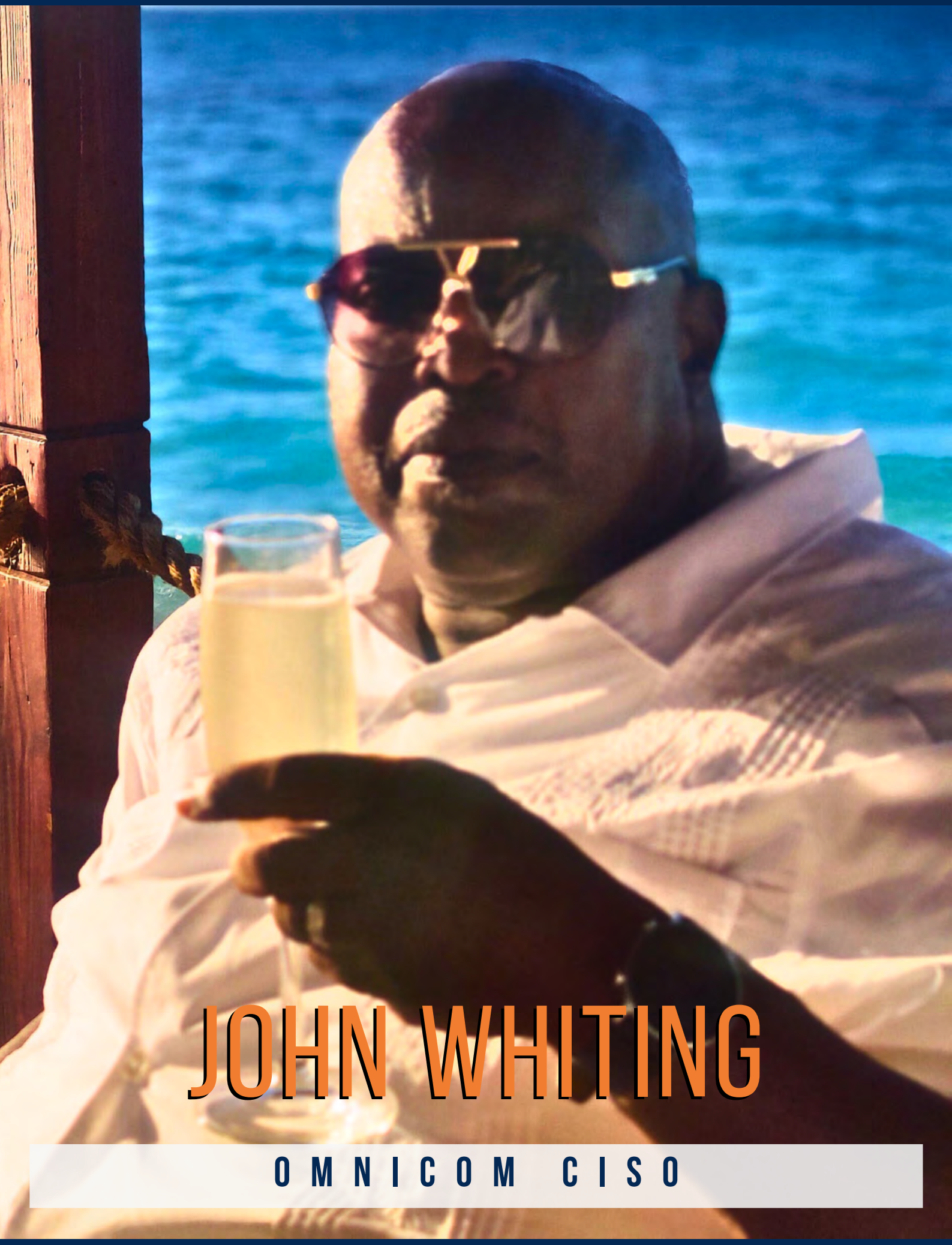
Work-life balance is important for Ross.

"I'm always encouraging my team to take time off to have fun. I love to do anything outdoors. I love to hike. I love to bike. I love to kayak. I have a second home in the mountains that we go to at every opportunity to relax and have fun. Plus, I'm always taking my Sheepadoodle to classes," she said.

"I also like snowshoeing. I like the thought of being that first imprint on the snow when it's purely white and no one's walked there before. That's kind of cool."

Volunteering is a big part of Ross's life. She's been on several boards of directors, including InfraGard, a partnership between U.S. businesses and the FBI; Women in Cybersecurity; Big Brothers Big Sisters; the Red Cross; and the Bucks County Council for the Arts.

"Some of my soft skills I think I got from being on these boards because you're around all different people from different backgrounds, and you're constantly negotiating and reading contracts and hiring staff and making decisions," Ross said. "I learn as much from mentoring as the person I'm mentoring or coaching."



JOHN WHITING

OMNICOM CISO

Don't be afraid of failure! That's a key trait that a successful CISO must possess, says John Whiting, the Global Director of Cyber Risk at global advertising giant Omnicom.

"Not every aspect of your program will succeed at first due to a variety of factors, such as technical, culture and support," Whiting said. "It could take years before an adoption of what you're trying to maturate in your program gets truly baked into the culture.

"The CISO is a rough role, depending on which organization you actually report to. If you report into technology, and the company is just starting their security journey, you may have the challenges – especially on the cyber end – of telling your boss that stuff under their management is not secure and needs to be fixed. If you report to the CEO or into legal, you'll probably have more compliance and audit support natively behind you. So depending on where you report to in the company may help or not help the journey of your success, depending on the industry you're in."

Other traits that contribute to a CISO's success are soft skills, like being able to communicate and convey your program to peers; being attentive to the needs and growth of your staff; knowing how to manage risk; and being knowledgeable about the organizational goals and aligning your program with them, Whiting said.

"You need to be involved as a risk manager, managing the cyber risk of the company, from security operations to architecture, to threat intelligence, data governance, asset management and third parties. It's a holistic picture," he said.

A critical part of risk management is what you can mitigate and treat and when, and how you transfer or accept the residual risk for a documented period of time, he added.

Automation of intelligence and incident response, zero trust networking, identity governance and protecting APIs are the top industry trends he identifies.

Whiting leans on more than 20 years of experience in information security and technology. He was recruited to his current position from Omnicom subsidiary DDB Worldwide Communications Group, where he served as the first global chief security officer. Prior to that, he was the director of information security and inaugural business information security officer for Global Corporate at insurance powerhouse AIG.

Whiting served as director of IT and security at Publishers Clearing House at a time when the company was being sued over its promotional practices by attorney generals in all 50 states, making it a high-profile target for threat actors.

Whiting advises fledgling CISOs to have some overarching risk management experience, and soft people skills to deal with staff and colleagues. And lastly – "a lot of heart and passion to deal with finance and budgeting challenges," he said.

This multifaceted experience has informed his execution of the CISO role by making him operations oriented and business savvy.

"In some of the jobs I had, along with security, I was also responsible for resiliency and accountable for some operations. And I knew what it took to actually operationalize IT and business programs. And because I understood what it took to run the operations, it helped me in talking to constituents on a business level," he said. "That's very important these days with the evolution of the CISO, who is much more of a business leader and lobbyist than previously. I also understood about budget constraints and resourcing constraints and how to get stuff done.

"And because I worked at some very large companies that were older and methodical, I was able to transition the soft skills of having good operational manuals, runbooks and standard operating procedures to standardize and make repeatable processes that lead to better security. They're not security per se, but because it's driven in a systematic way that's repeatable, it's easier to audit and it's easier to control the security."

Staffing and having the budgets to retain good staff is the number one challenge facing CISOs today, Whiting said.

"There's always a resource shortage," Whiting said. "There's a lot of leaning on cross-training of other areas and talents, along with augmented staff. But the augmented staff is good for repeatable processes or under the guidance of full-time staff, because they do not have the legacy resident knowledge to help the process long term. Make sure your internal staff are happy and being developed. Take their input on improvements to the program and have them engaged with the constituents."

He presents his budgetary case by focusing on facts, risk and rewards rather than metrics.

Whiting advises fledgling CISOs to have some overarching risk management experience, and soft people skills to deal with staff and colleagues. And lastly – "a lot of heart and passion to deal with finance and budgeting challenges," he said.

He also warns them to prepare for the fact that they're going to get breached.

"Users and constituents are not going to always listen to you until after the fact," he said. "And you just need to remain calm and deal with that. That's part of the job of being a CISO. You are a counselor."

And when that breach happens, "never let that opportunity go by," he said with a laugh. "A good incident might be a point to leverage your program to get more people aligned with you and to get your budget in."

At Omnicom, Whiting is involved in every facet of the risk program, interfacing with dozens of teams and corporate to make sure all risks are addressed, and in compliance with regulatory requirements and control objectives. One focus is innovating the management of risk around emerging technologies such as artificial intelligence and robotic process automation as he develops more systematic control objectives to the new risk.

"Automation is the next thing, which is why stuff such as machine learning and AI are top on the list right now," he said. "The question is, how do we control those risks around them?

Whiting sees the CISO's role evolving in the direction of a subject matter expert and consultant.

"Most of your high-volume work, such as vulnerability management, security monitoring, pen testing and parts of your incident response, is all outsourceable to service providers," he said. "That leaves the CISO more time to evaluate the data and the metrics outside of those and evaluate the risk, while at the same time becoming more of an advocate to the business instead of spending your time or your staff's time monitoring screens."

Whiting decompresses from the stress of his work with hobbies – classic cars, a passion for cigars (mostly Nicaraguan, Cuban and Dominican), and travel.

"I travel all over the world. I love the Caribbean and I love Europe," he said.

SHIFTING GEARS

FROM ENTERPRISES TO CHALLENGES BEYOND

DEVON BRYAN

LIFE AFTER BEING A CISO

CARNIVAL CORPORATION, CHIEF INFORMATION OFFICER

Becoming a chief information officer or chief technology officer was something Devon Bryan aspired to as a longer-term career objective. He didn't imagine it would happen so soon.

"As I was eyeing life after being a CISO, I was certainly considering making that transition at some point during my career," said Bryan, who was appointed Global Chief Information Officer at Carnival Corporation in December, after just 15 months as the cruise operator's Chief Information Security Officer.

"But the opportunity presented itself a lot sooner than I expected, and it was a tremendous opportunity to help drive the global IT strategies for a wonderful organization."

Skills Bryan had developed as a five-time Chief Information Security Officer definitely lent themselves to his stepping into the role, he said: technical and business acumen; exposure to cross-organizational key business processes and applications; strategic thinking; risk management and an innovation mindset.

But even before that, 11 ½ years on active duty in the United States Air Force instilled formative lessons about organizational leadership and people leadership that have directly translated to his post-military career overall.

"Mission first, people always. Being a good teammate and a team player. These certainly have been some of the important military doctrines that I have internalized in my career in the private sector, and I believe they have served me well," Bryan said.

CISOs and CIOs can have conflicting agendas, as he knows from personal experience: He quit one CISO job because the company's CIO was presenting overly rosy pictures to the board, what's known as "The Green Dashboard Syndrome."

"I actually have a fantastic partnership with my current CISO!" Bryan said. "Having walked a mile in her shoes as a former practitioner, it would be absolutely nuts for me to engender an organization where there's conflict between my CISO and myself. "

The "natural and healthy" tension that comes from the CIO-to-CISO relationship can be managed with frank and fair conversations, he said.

"By establishing trust, by having honest, open, transparent communications and collaborations, that conflict can be managed, mitigated into being healthy versus unhealthy. Healthy conflict is the operative phrase here."

Bryan joined Carnival more than two years ago as the cruise industry, clobbered by the Covid pandemic, was getting back into the water. It was his first foray into the travel and tourism industry, after having spent most of his 25-year cybersecurity career in and around the U.S. financial services sector.

He reported to Carnival's board in his former capacity as CISO, but now, his conversation with board members is more focused on IT as a core business enabler.

"Arguably every company is an IT company disguised as something else since IT underpins so much of what business does, irrespective of industry vertical," Bryan said.

His strategic pillars include better leveraging IT investments to drive top line revenue growth, reduce operating expenses, enhance the guest experience, and improve employee productivity.

Transitioning to the CIO role has required adjustment on multiple fronts.

"It's a different environment from being a CISO. What conferences do I go to? What CIO groups do I participate in? Where am I getting my information? What information should I be focused on now?" Bryan said.

"I am no longer the CISO. I have to defer a lot of these vendor calls and vendor dinners and a lot of these security conferences to my CISO, so I can focus on the more technology-focused and business-focused events. I'm having to grow new muscles in multiple ways."

The company's structure also poses a different dynamic.

Carnival is a matrix organization with nine industry-leading cruise line brands, including Carnival Cruise Line, Cunard, Princess, Holland America and Seabourn, AIDA, Costa, P&O Cruises UK and P&O Cruises Australia. Bryan is the CIO of the CIOs for the respective brands, but the CIOs or CIO equivalents at the various brands do not directly report into him, making the executive core competencies of influencing, negotiating and being able to collaborate across diverse organization boundaries critical to his success.

"If I'm not able to collaborate, I won't be successful," he said. "So that is a unique challenge to me in this role."

But Bryan has encountered this type of organizational structure before.

His first big job out of the military was at the Internal Revenue Service, where he helped to create the agency's first security operations center. There, he had to navigate the complexities of a 110,000-person organization to deliver cyber priorities. Most of the initiatives were compliance driven, but in a sharp departure from the military, there was no four-star general in a hierarchical structure giving orders.

"The IRS was where I really got perhaps my first exposure to the importance of being able to influence, to negotiate across a large organization in a matrix fashion, and get work done through others, not based on command authority, but based on the power of persuasion," he said. "That was certainly quite a learning experience for me."

He had a similar experience during his tenure as the System CISO for the National IT Organization of the Federal Reserve System, where he had to collaborate with the CISOs of the Fed's 12 regional banks to align on priorities and strategies to secure the nation's central banking infrastructures.

The senior leadership team of Carnival has been very supportive in his current role, Bryan said. He also turns to people outside the organization, former CIOs who volunteered their services to help him succeed.

"I feel so very supported by the community as well as by the company," he said. "I've always viewed mentorship as being critical to the success of technology practitioners. Mentoring is critical, not only to give back, but also to further develop and advance your practitionership and leadership."

That belief led Bryan to co-found Cyversity, an organization dedicated to achieving a diverse and inclusive cybersecurity workforce through scholarship opportunities, diverse workforce development, outreach and mentoring programs.

"We wanted to just do the little that we could to leave the industry a lot more diverse than we found it, because there's not enough women, and there's not enough black and brown practitioners," he said.

When he's not at work, Bryan is usually reading or volunteering with Cyversity, but he has also been learning to play the guitar; Afro Jazz and Reggae are his favorite forms of music. He's also learning to play golf, and is working on a handbook for CISOs in the early to mid-stage of their careers.

People who transition from the CISO role like he's done have a range of opportunities available to them. The next evolution of CISOs will depend in large part on what an individual wants to do, Bryan said.

"We've had folks who transitioned into the CIO role like I did. It's very separate and distinct from a CTO role, but that's also another career path. And we've had folks who've gone on to be venture capitalists or work for vendors, and others who have gone straight into doing boards. And of course, folks have also opted to go into academia and teach.

"The life-after-CISO chapter has been shown to take a number of different twists and turns," he said. "But the calculus for each of these decisions is very varied and very personal."

BENJAMIN CORLL

LIFE AFTER BEING AN END-USER ENTERPRISE CISO

ZSCALER CISO

Benjamin Corll's transition to vendor CISO from enterprise CISO wasn't anything he'd been aiming for. But when a great opportunity came his way, he took the leap.

"Opportunities are abundant if you're willing to look for them or see them as an opportunity," said Corll, now CISO in Residence at cloud security company Zscaler.

"I was a customer of Zscaler for five years. My last enterprise job was in manufacturing, which was a fantastic role for me at the time. But I wanted to move back to more of a technology-based company, a forward-thinking type of organization. And as a customer, I really liked my engagements with the senior leadership of Zscaler. It was an interesting role, so I moved over."

The forward-looking aspect played a big part in his decision.

Corll, who got his start in information technology as a small computers specialist in the Marine Corps, built security programs for 25 years. But while some CISOs of his generation have stuck to the same hub-and-spoke format they used when starting out, times have changed, and so must the approach to security, he said.

"Some of the most dangerous words you can say are, 'We've always done it this way, but I've been successful,'" he said. "Our adversaries have changed, and technology has changed.

"I joined Zscaler because I really do believe that to be successful into the future, we're going to have to adopt this concept of zero trust. And Zscaler is on the forefront of that."

Corll was offered the job after impressing Zscaler with a customer testimonial at the company's annual conference. In this role, he engages with customers and prospects, writes articles, and speaks at conferences.

But while he isn't directly involved in Zscaler's security program, he and his teammates take a lot of the burden off of the enterprise CISO by talking to prospects, and working through their contracts and security questionnaires, he said.

And as a former customer, he can have conversations with product management about his personal experience with the platform and suggest possible tweaks or different perspectives. He also supplies product management with customer feedback.

Advocating for customers makes the product better, he said.

"My counterparts and I were all CISOs as customers in our previous lives, so it's not just sales jargon," he said. "I really advocate for our customers. It's not an 'us versus them.'"

Corll takes exception to the notion that he's "gone over to the dark side."

"One of the shocking things that I experienced was the number of CISOs who would say that to me," he said. "That really bothered me because we're supposed to be working on the same side. We're working against the adversaries. *They* are the dark side. If we want our vendor partnerships to be better, isn't going to work for a vendor a logical place to go?"

"I was really surprised that I was no longer eligible for membership in some of the groups that I had been in before because they no longer consider me objective," he said. "It's like you're tainted. It's insulting."

Corll has been at Zscaler for a year now, and the transition has involved a culture shift. The pace is much faster. He's in more of an advisory role, and doesn't manage a team. He also doesn't have human resources responsibilities.

The new role has also given him an opportunity to cultivate softer skills, like focusing on telling a more compelling story.

"It's been great pushing that keyboard a little bit further away and focusing on relationship-building, focusing a little bit more on the presentation skills, and getting a little bit more dedicated time to focus on authoring some articles," he said.

And the work-life balance is better.

"I do get to stop the day at a set time, and if things hit the fan, it's unlikely that I'm going to get called in," Corll said. "I don't have that fear that at 2 o'clock in the morning, I'm going to get the call that ransomware is spreading around on my network."

At the same time, he does miss the camaraderie of building a program together with a team, and the kinship that comes with working in the trenches together. He also misses the type of strategic thinking required to put together roadmaps – especially the longer-term ones that involve technology that hasn't even been invented yet.

"I may jump back in and build another security program at some point in the future if the right opportunity arises," he said.

Corll is also looking for opportunities to train the next generation, and "give back to a community that has given so much to me."

"I needed that mentor years ago, and I like training others and helping others. It makes me feel good when I can help somebody else," he said.

Right now he's directly mentoring several people.

"That first role is extremely difficult. So I like to sit down with people, virtually and physically, and walk them through how they need to present themselves, and the training they should have," he said.

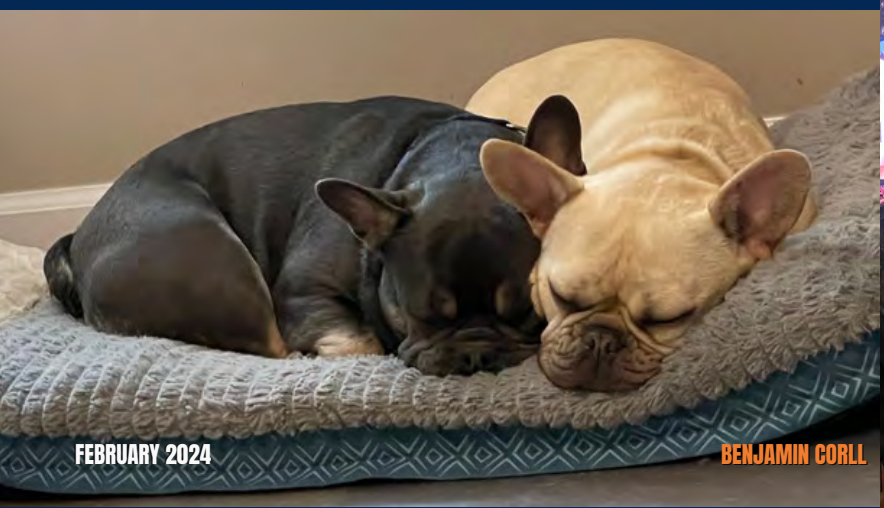
"After they get a little bit of polish, I start using the professional network to make some introductions, after understanding what area of cyber they're interested in."

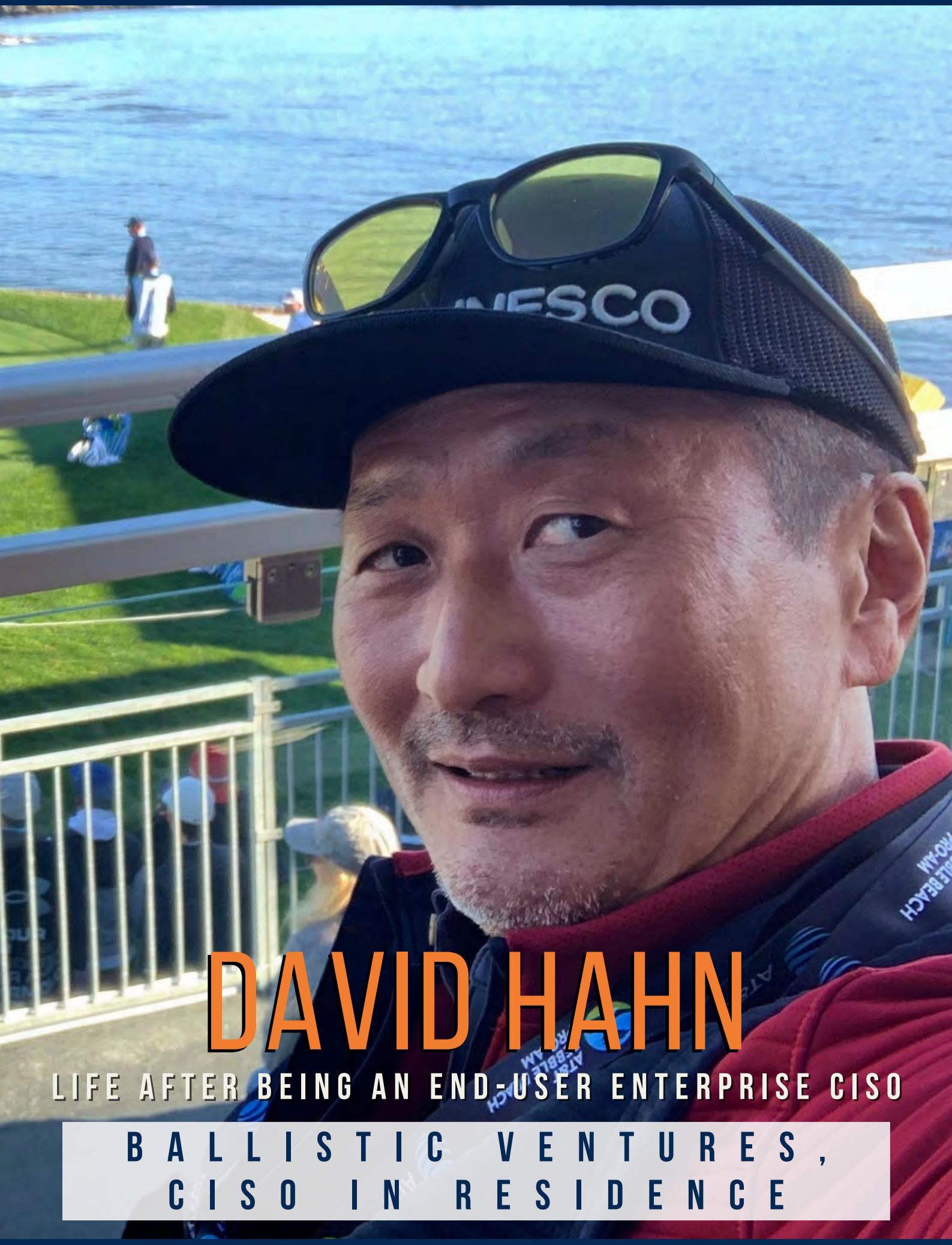
In another expression of his desire to give back, Corll is a board member of Join the Journey, an organization that gives microloans to businesses that would not be able to find other sources of funding.

"They give microloans to women in Zambia, and it allows them to start a business," he said. "So it changes their lives. It betters the lives of their families and their communities.

"When I learned about the organization, I knew I had to go help there. I wanted to be more actively engaged than just throwing money at it. I wanted to employ skills I have learned in life to help this organization have a greater impact.

"I've only been with them 18 months, but it's been long enough to truly believe in the vision."





DAVID HAHN

LIFE AFTER BEING AN END-USER ENTERPRISE CISO

BALLISTIC VENTURES, CISO IN RESIDENCE

David Hahn describes himself as a security evangelist.

"I think security should be very democratized," said Hahn, the inaugural CISO in residence at Ballistic Ventures. "Part of a CISO's job is to evangelize and to really get people – from board members all the way down – to understand what security is and what they need to do to protect the company."

A CISO's staff is not only their team, but the entire company, he said.

"Everybody in my company is a security person," he said. "They have a role to play and can always learn more. We want them to feel both engaged and empowered to protect the company. That's the only way that we can scale across, and we need everybody to get to be a security person."

Before joining Ballistic, Hahn worked for CDK, a leading retail automotive technology developer; Silicon Valley Bank, a specialized lender focusing on startups; the Hearst Corp., and and Intuit, a Silicon Valley financial software company. His longest career stint – 23 years – was at Wells Fargo Bank, where he started as manager of employee benefits and investment plans, and wrapped up as senior vice president and information security officer for the internet services group.

"When I started working out of college, the internet was just getting started. I certainly didn't know what I wanted to do back then," he said. "But everything I have done I have taken into subsequent roles: business acumen, solving problems, working with difficult people and complex situations, dealing with large-scale size."

Today, the CISO's role has evolved to take much more of a risk-based approach. CISOs have to learn what's most important to their company and how to put in controls that protect data, its integrity and its availability, while enabling the business to grow, he said.

"You're going to have a hard time being one unless you have the business acumen and understand that you cannot just rely on your technical background or competence," he said.

"You can be successful by solving complex problems, by working on bringing people together," he said. "As CISO, you get involved in all aspects of what your company is doing, and get to speak to just about everybody, because everybody has some kind of security issue. You have to have that ability to work across different levels of management and positions, trying to get people to understand what the risks are for each of them."

During his 15 years in the infosec trenches, Hahn spent a lot of time with startups and people in the venture capital world, and the idea of crossing over to that segment of the security industry intrigued him. So when Ballistic Ventures offered him the opportunity to become its inaugural CISO in residence, the time seemed ripe to make a move.

"I wanted to get more involved in the investment world and see what that was like, see the other side of the glass, so to say," he said. "If you have been a CISO for, let's say, 15 years, which I have, you start to see that just about every company's got the same kind of problems, no matter what the industry. So you're looking for something different. And the stress and pressure that you're under as a CISO is wearing.

""You can certainly take your passion and extend it without having to be a so-called operator all the time," he added. "For me, this was a great chance to divert a little bit. You need to get a fresh perspective, and I think I'm getting that now."

For years, Hahn was a marathon runner, and he can see analogies between running endurance races and working as a CISO.

"It's not a sprint, it's a marathon," he said. "You have to be patient as well as endure. You have to live through lots of pain. You have to be relaxed. There are a lot of pieces you can draw together. You create wear and tear. It's also a little bit crazy, and something you have to commit to. So there's a lot of little things you can correlate."

While he's scaled back distances, Hahn is still running, heading out several times a week.

"It's mental relief. I've been doing it my whole life. Blank out, zone out, listen to things. I used to listen to music, now I listen to books. It's a good way to destress yourself from the day, and then I go home and take a shower and have a glass of wine. You need a routine, but also an outlet to separate yourself from work. You can't do it 24 hours a day."

The biggest challenge in a CISO's job are the many competing priorities that a business has to face, he said.

"For a CISO to be successful, you have to be part of the conversation of where the business priorities are, and not somebody who says don't do anything. You're never going to enable the business that way," he said.

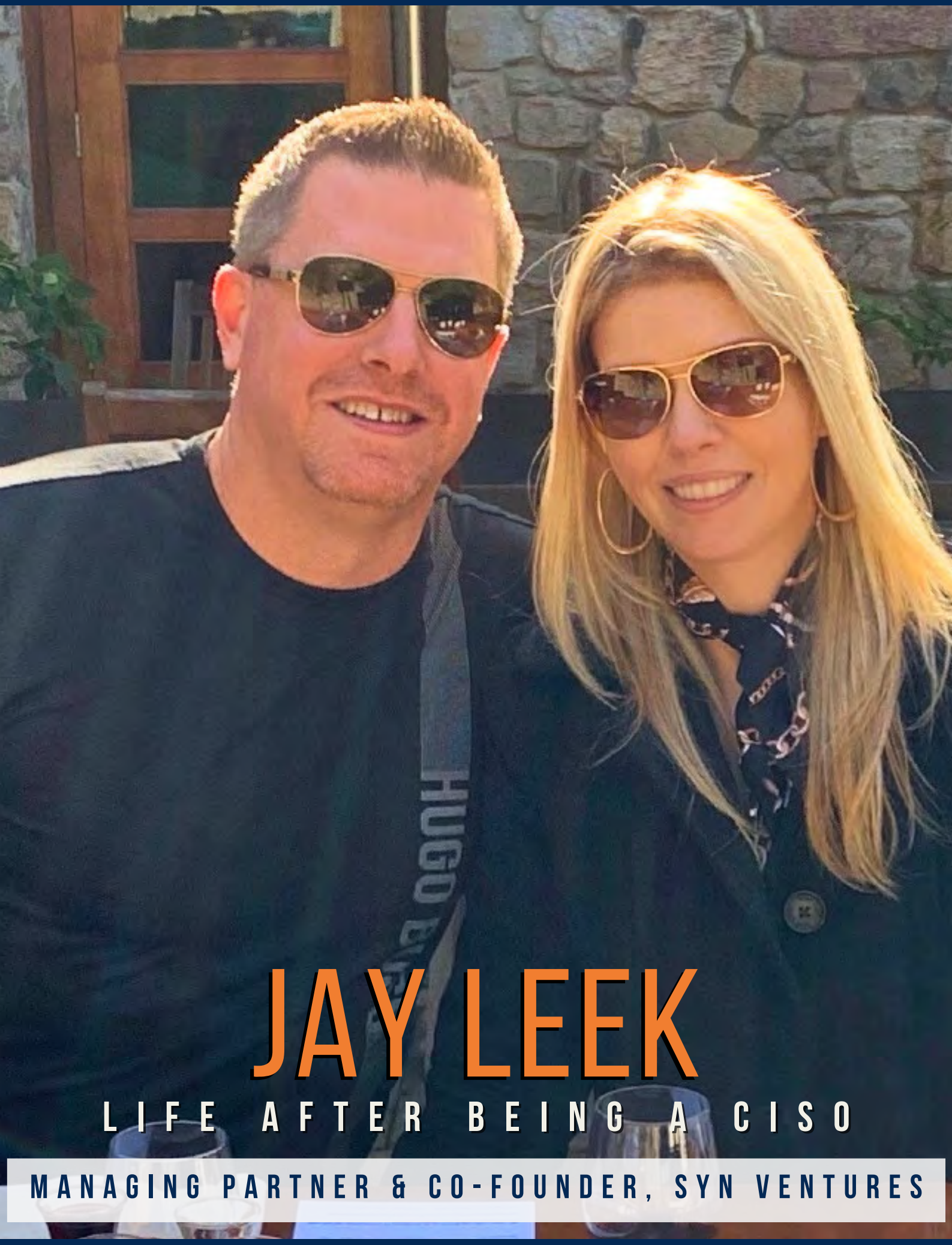
"You have to explain what the risks are, but you also have to be able to help the business accept certain risks. You can never be at a point where there will be zero risk. If you approach things that way, you'll probably be overspending and not doing enough to move the business forward. A good CISO can help a business make good decisions on taking risks."

Hahn makes it a point to look at business trends, not just specific trends in cyber.

"It's all about how companies are changing the way they work," he said. "Security people have to be at every one of these things to be able to figure out how to protect data, its availability, and its integrity."

His advice to people just entering the field: Don't worry so much about the end position or the title.

"Instead, make sure you have a curious mindset and that you want to learn. And if you do that, things open up," he said. "Always be curious about understanding how things work, and be good at what you do. If you're good at it, you will actually enjoy it. Get involved and ask questions so you can learn from there. Learning is so important."



JAY LEEK

LIFE AFTER BEING A CISO

MANAGING PARTNER & CO-FOUNDER, SYN VENTURES

The startup world fascinated Jay Leek when he worked as Chief Information Security Officer at some of the world's biggest companies. The former Blackstone CISO and senior security executive at Nokia and Equifax has parlayed that fascination into a thriving new career as a cybersecurity investor.

"I based my career on embracing emerging early stage startups in my security program because that's the only way you can really innovate," said Leek, now the managing partner and co-founder of SYN Ventures and the ClearSky Security Fund. "I'm not knocking the big guys, and there's a place for them as well, but innovation's happening in the startup world."

The inflection point came at Blackstone, where he cultivated a hybrid role as full-time CISO, with key responsibilities for early stage cybersecurity investing, and working with private equity on leveraged buyouts in cybersecurity.

"In my last 18 to 24 months there, I was probably spending the majority of my time more on the investment side," he said. "After 18 years of running security, the job shifted to value creation, having the opportunity to provide entrepreneurs with capital, sit on their boards and work with them.

"I could watch companies grow, instead of protecting something from getting torn down or watching something get torn down. I could see economic wealth be created, help solve unique problems that hadn't been solved before. And honestly, that was really what was getting me out of bed in the morning and really, really excited to go to work. So in 2016 I decided that I was going to leave."

Leek started ClearSky Security the following year, and SYN Ventures in 2021. His funds have raised just under a billion dollars and invested in 56 companies, and he has completed 25 exits. Over the past five years, his combined firms have been the most active cybersecurity investors in the world by deal count, and have had the second-most cybersecurity exits during that same period of time.

"The three pillars of our investment thesis have been efficiencies, automation and prevention first," he said.

A couple of his big wins include selling Cylance for $1.5 billion to Blackberry and selling Optiv Security to KKR for almost $2 billion. Leek also measures success by seeing investments accelerate businesses and create wealth for founders and employees.

He and his partner, Patrick Heim, are the only two former fortune 500 CISOs to have started a venture partnership. Their inside track on CISOs' pain points is part of what has made them so successful, he said.

"We've made sure that we are still hyperconnected to the CISO community," he said. "We have a CISO board of advisers, and a broader group of CISOs we work with," he said. "We think very much about our investment strategy as if we were still running security for a Fortune 500 company."

"Get active in companies, help the company, help create value. That'll give you good visibility and prep work to go sit on a board of a company and help add a lot of value. You've got to serve on boards and understand what it's like to do that before you can really understand what it's like to be an investor."

The ongoing connection with the CISO community has created a "fantastic" symbiosis, he said.

"We help them by helping CISOs think through problems they have, and they help us keep our finger on the pulse of the real world problems that people are facing today, and not the problems we faced five years ago," he said. "That's how we stay fresh and current, and that obviously helps to inform our investment thesis and helps it stay current."

Given the talent shortage in the industry, Leek expects Fortune 500 or Global 200 companies will eventually use a next-generation piece of technology to address an issue or risk.

Shifting attack modes are also playing a major role in his funds' investments. With adversaries using technology to attack, companies need software speed and response, he said.

"Take ransomware. A human is not going to go blocking and tackling to prevent that. You need real prevention in place actively with software to get ahead of that," he said.

Many former CISOs aspire to invest, but "unless you have the opportunity to really get exposed to it beforehand, it can be very dangerous," Leek said.

"Also, making individual investments in individual companies versus at a fund level is very different," he added. "It's hard to have the resources as an individual to really make a difference and influence those investments the way you need to, versus having fund resources behind you, as we do."

CISOs interested in getting into investing should get active in advisory board work so they can get on boards, he advised.

"Don't be an advisory board member who's just leasing out your name for marketing purposes," Leek said. "Get active in companies, help the company, help create value. That'll give you good visibility and prep work to go sit on a board of a company and help add a lot of value. You've got to serve on boards and understand what it's like to do that before you can really understand what it's like to be an investor."

While leaving the operational side of cybersecurity has given Leek more control of his time, it hasn't given him more free time.

"I'm not as worried about a certain nation-state creating problems for me, but I do have 35+ CEOs running around with money that investors have graciously trusted me to invest on their behalf, and that comes with its challenges too," he said.

"I know a lot of folks who want to leave the CISO profession and want to work three or four days a week, and disappear for a week if they want to. I don't have that luxury with the decision I made."

When he does have free time, wine plays a major role in his off-work life.

"My wife and I collect wine, so pretty much all of our vacations revolve around wine, visiting wine spots around the world and doing wine tours and tastings and things of that nature," Leek said. "We just love Barolo and Bordeaux, and we usually like an Old World style versus the New World."

Leek breaks down CISOs into two categories: Those who are good at running things, and those who are builders.

"There are those who are great at running the firm, and that is great and much needed. They are more operationally driven," he said.

"I'm a builder. That's probably why I invest in startups, too. If you're on the builder side, you've got to be very entrepreneurial. You've got to figure out how to push limits, but not push too hard. And you've got to take risks."

KARL MATTSON

LIFE AFTER BEING AN END-USER ENTERPRISE CISO

NONAME SECURITY FIELD CISO

Karl Mattson was at his third financial services firm when he realized it was time for something new.

“I found the pattern was familiar, and wasn’t bringing the best version of myself to work every day. I needed a new kind of challenge,” said Mattson, who for the past two years has been CISO at Noname Security, a developer of technology that detects and blocks API attacks.

“CISO roles in financial services are extremely difficult. I would never suggest that I had mastered it by any stretch. But there was a little bit of a burnout factor, and I needed a change of scenery, so to speak, to a new kind of challenge.”

Mattson had known Noname’s founders as a very early customer, so that eased the transition.

“In those early days, Noname was a very small company, so I knew everybody there,” he said. “So for me to join Noname didn’t feel like a risk or unknown because I knew the team, and I knew the platform very well. So it was a very natural fit for me to take the role.”

He landed the job while trying to find others to fill it.

“Originally the CEO asked me for advice on hiring a CISO. I introduced him to a couple of people he interviewed. But in the end, there were various factors that all supported me being a great fit for the company, and the company being a great fit for me.”

“The missing ingredient for success is not commonly a technical issue,” he said. “It’s more commonly a discussion about how we can make this simple for the customer so we’re not adding more work, that we’re actually making life easier and better.”

Mattson got involved in cybersecurity straight out of high school, when he joined the Army and was assigned to be an intelligence analyst at the National Security Agency. After about a decade there, he transitioned to the corporate sector, ultimately winning CISO roles in the financial sector. At Noname, he has dual internal CISO and public-facing CISO responsibilities.

In the latter role, his primary brief is to educate the general security community about APIs and associated risks. He does conferences and keynotes, and networks with CISO peers to build and maintain a customer base. He also runs a 20-member CISOs advisory board for Noname.

“The opportunity of joining a startup early in its lifecycle is an all-hands-on-deck experience every day,” Mattson said. “By helping to build essentially from a blank whiteboard, that really taps into everything that I have as a professional to offer.

“Everybody has to wear every hat all the time while you’re in a growth phase, whether it’s doing financial budgeting or helping recruit new engineers, or trying to pick out an office space,” he added. “The great thing about working for a startup is that you get to touch and feel everything. You participate in all facets of the business. In a startup, if it’s not there and you need it, you have to build it yourself.”

Mattson’s experience in large enterprises trained him to understand what Noname’s customers expect from a security vendor “because I was that customer for a decade,” he said.

“I can tailor my focus to making sure that we’re doing things at Noname that are in line with exactly what our customers expect. I can put myself in the customer’s shoes very quickly and help us calibrate to make sure that we’re hitting the mark for the customer.”

Not all prospective customers have enough staff or skilled enough staff to adopt Noname’s software, so the biggest challenge is to make it as easy as possible to use, and to equip teams to be successful by enabling them to use the technology, he said.

“The missing ingredient for success is not commonly a technical issue,” he said. “It’s more commonly a discussion about how we can make this simple for the customer so we’re not adding more work, that we’re actually making life easier and better.”

Mattson expects to see more CISOs shift into related roles in the security ecosystem.

“There are a significant number of CISOs who are at points of their career where they’re experiencing burnout or their resources are limited, and they have a mission that almost feels impossible,” he said. “More and more CISOs are looking at adjacent career moves, whether to a vendor or a VC firm, or an advisory role.

“We need to embrace being a farm system of talent, and to promote the healthy circulation of talent.”

The ability to manage talent is the No. 1 skill a CISO needs, Mattson said.

“Attracting and equipping and retaining key talent in an organization will be overwhelmingly the most important thing a CISO can do for the organization’s health and security,” he said.

“Then we start on prioritizing risk, prioritizing budget, and managing the department’s resources to maximize the risk reduction. The other part is business enablement: How do we position the security organization as an asset to an organization rather than a cost center. That’s an important facet.”

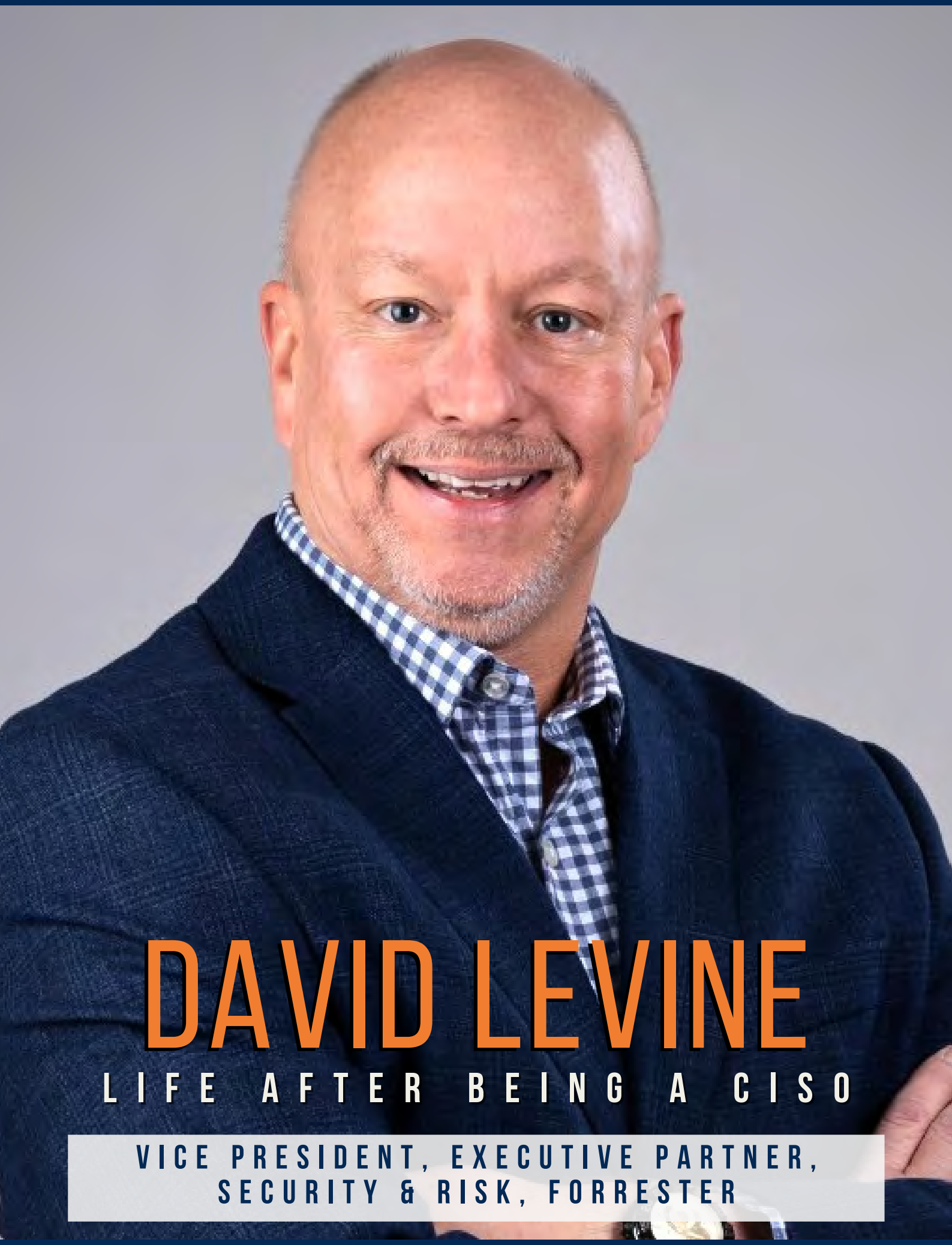
In the eight years since he first became a CISO, Mattson has seen the role assume an increasingly higher profile. The inclusion of CISOs in major business strategies and major decisions on risk isn't related only to cyber risk, but to broader business risk, and that's a trend he expects to continue. He also sees information security becoming more autonomous, modeling trends already underway in financial services - a development he hopes will expand to other sectors.

Mattson sees an analogy between the role of a sports coach and that of a CISO.

"You bring your people in and you bring your playbook in, and you're kind of fired up for a while, but after a few years, a good coach will recognize that it may be time to move on to another college or another team," he said. "And then they get a burst of energy to start the journey all over again. The natural lifetime of a CISO is three to five years. It's so rare that people can still be effective in their role after so many years keeping up the pace, and maintaining the attention of the organization."

That said, Mattson "absolutely" sees himself going back to the pure CISO role some day.

"I enjoy a startup organization, but I also look back at some of the larger teams that I've had the opportunity to lead and be part of, and that was also rewarding," he said. "I've got a couple of stops in my career left. If things go well, I'd like to go back to a large enterprise, I'd like to be an investor, and do all of the above one more time."



DAVID LEVINE

LIFE AFTER BEING A CISO

VICE PRESIDENT, EXECUTIVE PARTNER,
SECURITY & RISK, FORRESTER

As the inaugural security and risk executive partner at the Forrester Research and Consulting company, David Levine marshals his vast experience in cybersecurity to counsel industry practitioners.

"With security and risk being what they are, and the CISO continuing to gain in importance at companies, Forrester thought it would be a really good fit to bring somebody in to pair with customers who are security practitioners, and the demand is there," Levine explained.

"Most of my clients are CISOs or high-level security leaders," he said. "We meet with our clients on a regular cadence to provide guidance and act as a sounding board, in much the same way that I leaned on the CISO community when I was an active CISO. It's really a way to take that same concept and formalize it in a way that affords consistent interaction."

The new job has given him an opportunity to learn about different industries and areas that he wouldn't have been exposed to in detail at Ricoh USA, Inc., the Japanese multinational imaging and electronics company where he forged his long security career.

"In one sense it's a different ball game because different things guide their efforts," he said. "But at the end of the day, the job of being a CISO is the job of being a CISO, no matter what job or industry you're in. The core role and the things that CISOs should be doing to be successful doesn't change. But it's been really fun working in a lot of different areas and being exposed to new things."

One of the many current themes that Forrester continues to dive into is CISO and team burnout.

"The pressures are crazy," Levine said.

"You've got to be in the business, with the business, and moving the business forward. You also have to move your own projects and priorities along all the time, while dealing with issues that pop up, and incidents that may happen. And you have to get it right all the time, because the adversaries never stop. So there's a lot going on, and I don't know many CISOs who claim they have enough people and enough money, and that adds pressure, too."

The accountability issue that emerged from the high-profile Uber data breach case has also entered the industry's conversation, he said. For all these reasons, Levine definitely expects to see growing numbers of CISOs seek other types of jobs that will keep them connected to security, but without all the day-to-day pressures that weigh on an active Chief Information Security Officer.

"I think you do have people who are going to say, 'Hey, I love security, but maybe I want to find something that's a little different,'" he said. "Companies are going to have to figure out burnout. It's already a problem, but it's going to continue to be an even bigger problem."

That's where leadership comes in, Levine said.

"There are some very fundamental things you can do as a leader that aren't hard and aren't complicated but can make a big difference. And it all boils down to one rule: Be the leader you would want."

Before starting at Forrester late last year, Levine had spent nearly 30 years at Ricoh in various capacities, including a decade as CISO.

"It was tough leaving my team," he said. "We broke the mold in a lot of ways. First of all, I was a CISO in the same place for 10 years. That's almost unheard of. What's more, the tenure in my team at Ricoh was crazy. I had people who were there almost as long as I was, some longer, and a whole lot that still were way above and beyond the average. So it was really hard to leave those folks as we were a pretty tight-knit team."

"Ultimately part of it just came down to that I had been there so long, and while I was really proud of what we accomplished and built, it was a good time to hand over the reins. And I liked the idea of doing something a little different, and trying to see if I couldn't capitalize on the things I really enjoyed doing the most. I became really involved in the CISO community over the last several years, enjoyed the consulting aspects of what I was doing along with writing and speaking, and so being able to take that and run with it at Forrester was really appealing."

Finding himself at a new place after so many years came with some adjustments.

“I kind of had to laugh at myself sometimes because you get so ingrained in doing things a certain way,” Levine said. “I was like, ‘Oh, this is all different.’

“Making that transition from a leader with a team to individual contributor was a bit of an adjustment as well,” he added. “But I am blessed to work with so many amazing and talented people at Forrester that push my thinking and challenge me on a daily basis. “

One of the advantages of his current job is that he doesn’t have to be “on” all the time.

“I don’t miss my phone ringing in the middle of the night or getting that phone call on Thanksgiving or New Year’s or Christmas Eve,” he said.

On a personal note, Levine now has a greater opportunity to pursue a passion he’s developed in recent years – running.

“I started running in 2019 and it’s really turned into something I enjoy. So I try to run a competitive 5k every weekend if I can,” he said.

He’s also served in the Georgia State Defense Force for the past 8 ½ years, and describes himself as a “big, big car guy.”

“I like working on cars and fabricating. I used to do a lot of track days and even raced one season. I stepped away from that not long ago, but I’ll always be a car guy. You can frequently find me wrenching in the garage. I honestly enjoy that aspect as much I do driving.”