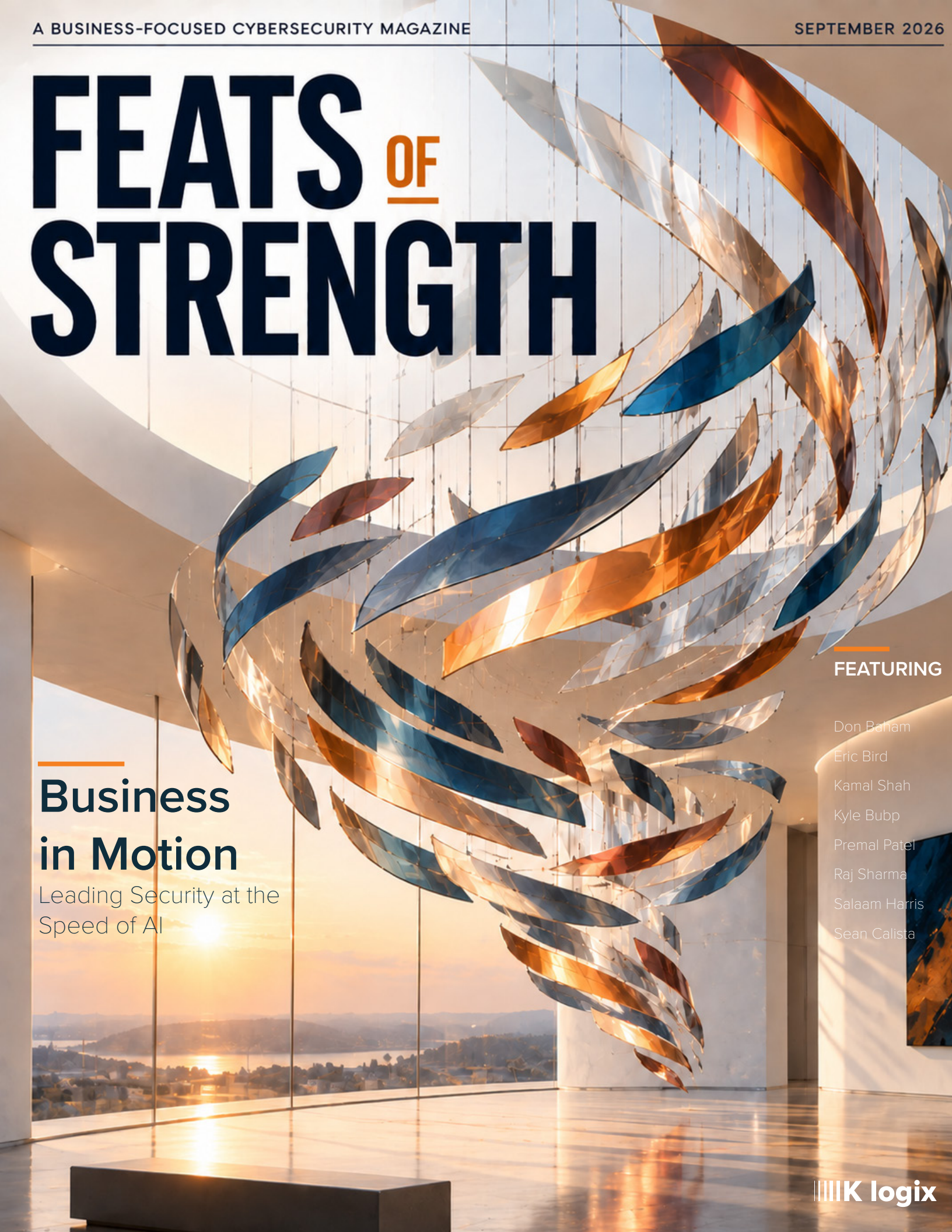
A BUSINESS-FOCUSED CYBERSECURITY MAGAZINE SEPTEMBER 2026

FEATS OF STRENGTH



Business in Motion

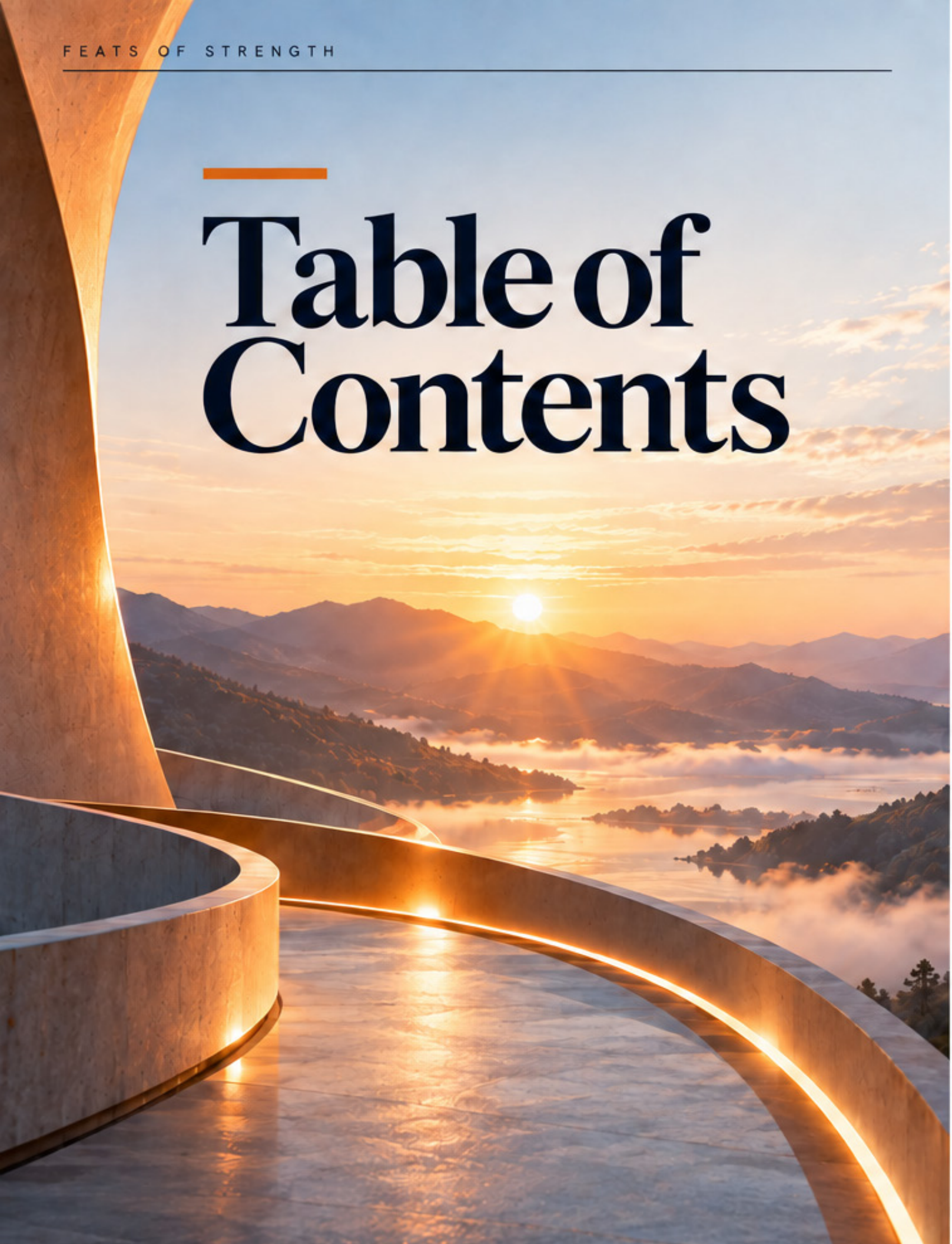
Leading Security at the Speed of AI

FEATURING

Don Baham
Eric Bird
Kamal Shah
Kyle Bubp
Premal Patel
Raj Sharma
Salaam Harris
Sean Calista

K logix

Table of Contents



PROFILES IN *Confidence*

DON BAHAM

CHIEF INFORMATION & SECURITY OFFICER

Rubicon Founders

Headquarters: Nashville, TN

Employees: 50+

Annual Revenue: Privately Held Company

Don Baham began his career in system administration, working across computers, servers, and networks before expanding into more client-facing positions. Over time, he moved between technical and more business focused roles, including professional services, sales engineering, and software training. That range of experience gave him an early ability to understand technology while also communicating its value to stakeholders.

"I enjoyed working with clients and being out in front, but I also enjoyed the technical side of things," Don recalls. "I think that has helped me throughout my career."

His path into cybersecurity came while working for a managed service provider, where a manager gave him the opportunity to take on security related responsibilities. He started with penetration testing, red teaming, and social engineering, gaining firsthand experience testing organizations from an attacker's perspective.

From there, Don's career increasingly moved toward security leadership and program building, setting the foundation for the work he leads today.

A PASSION FOR BUILDING

As Don gained experience, his career began shifting toward leadership. He started managing small teams and quickly discovered that developing people was something he genuinely enjoyed.

"The thing about leading people is that you don't really know if you're going to enjoy it until you do it," he reflects. "I started doing it with small teams and found I really loved investing in the team, team culture, company culture, and the next generation."

For approximately 15 years, people leadership has remained an important part of his career. At the same time, another pattern began to emerge. Don was repeatedly drawn to organizations undergoing transformation or acquisition, where he could help create something rather than simply maintain what was already there.

"I'm not really a maintainer," Don explains. "I'm a builder. I like to build things. I like to mature and grow programs. I'm not really one to come in and take over and just sit on the program. So, this is an environment that suits my style."

BUILDING SECURITY ACROSS A PORTFOLIO

Today, Don serves as Chief Information and Security Officer at Rubicon Founders, where his responsibilities extend across approximately 15 portfolio companies. With Rubicon both investing in and launching businesses, his role gives him the opportunity to build security and technology programs at very different stages of maturity.

For newly formed companies, Don is involved from the beginning, helping establish the technology architecture and security program while guiding key platform decisions. His team provides that foundation until the organization is ready to bring in its own leadership or transition day-to-day responsibilities to an outside partner.

As companies mature, Don's role shifts from building to advising. He works with technology leaders across the portfolio, creating opportunities to share resources and learn from one another while maintaining visibility into cyber risk across the fund. This allows Rubicon to identify where a company may need additional support and where greater maturity is required.

That foundation can be particularly important within healthcare. Some of Rubicon's companies begin with significant payer relationships, which means they may be handling sensitive information such as PHI. They do not have the luxury of waiting years for their security programs to

mature.

For Don, it is a model that plays directly into one of the strengths that has defined his career. Rather than maintaining a single established program, he is able to repeatedly build, strengthen, and potentially hand off programs designed to grow alongside the businesses they support.

CONNECTING SECURITY TO BUSINESS VALUE

Despite Don's technical background, his priorities today extend well beyond technology.

As Don's career has evolved, so has his view of the CISO role. Technical expertise remains important, but he believes security leaders must understand how their work supports the broader organization.

He explains, "At this point in my career it is about integrating with business operations, enabling the business, and translating what we are working on back to business value."

The fundamentals of security remain important, but Don believes a security organization becomes a strategic part of the business when it understands where the company is going and ensures its priorities support that direction.

FINDING THE RIGHT APPROACH TO AI

As Rubicon and its portfolio companies expand their use of AI, Don is focused on balancing responsible adoption with business value. As an investment firm regulated by the SEC with exposure to healthcare data, Rubicon must consider where sensitive information can go and which AI platforms are appropriate for different types of data.

For Don, that starts with governance and acceptable use policies with specific parameters around their different types of data. The goal is not to restrict adoption, Don explains, "We want to enable the business while reducing the risk that comes with broader AI use."

Now, he sees the conversation moving beyond access and toward value. Rubicon has enabled multiple generative AI platforms, but the more important question is what organizations are accomplishing with them.

"How do we actually use it to create value for the firm or for a portfolio company or both?" he asks. With organizations spending heavily on AI, Don believes measuring that investment against real business outcomes will become increasingly important. For him, that is the next stage of AI maturity: creating enough structure to use the technology responsibly while ensuring the investment is improving the business.

LEADING THROUGH TRUST

Don's approach to leadership has evolved considerably since he first began managing people. Early on, delegation did not come naturally. He admits that his instinct was often to handle something himself if he wanted to ensure it was done correctly. A mentor eventually showed him another approach, one that continues to influence how he leads today.

"The way I approach leadership is that it all starts and ends with trust," Don shares. "I try to empower the team to take on additional responsibilities that probably push them out of their comfort zone, and then give them the autonomy to go execute."

There is a balance to that autonomy as sometimes a leader needs to provide more direction or accountability. But Don has found that giving people room to work through challenges often produces better outcomes while creating opportunities for growth.

"More often than not, it allows team members to grow and create something or do something in a way that you hadn't thought of," he explains. "And that's fun and exciting to see how people solve problems."

"I'm trying to encourage people to experiment and learn how to figure things out, not just rely on a Google search, asking me a question, or asking Claude a question," he explains. "Go figure something out and come back with answers or some options. But I don't want to be the one feeding answers."

It is an approach built around giving people enough trust to stretch themselves, while remaining available to support them along the way.

CONTINUING TO GROW

Don holds himself to the same expectation for continued growth. "I moved from California to Nashville thirteen years ago and didn't know anybody. I started by getting into local associations and building my network," he recalls. "I'm an introvert by nature, but forcing myself to just get out there has helped me build a great network."

Today, Don participates in several national peer groups and has continued investing in formal executive education. Last year, he completed a Chief Information and Digital Officer certificate program through Carnegie Mellon and is currently preparing for another program focused on board leadership and executive development.

Today, the common thread is clear. Whether he is standing up security for a new portfolio company or evaluating how AI can create measurable value, Don continues to gravitate toward opportunities to build something better.

PROFILES IN *Confidence*

ERIC BIRD

PRINCIPAL ENGINEER, CLOUD, SYSTEMS, AND NETWORKS

ElevateBio

Headquarters: Waltham, MA

Employees: 344

Annual Revenue: Privately Held Company

Eric Bird's career has grown from the help desk through systems and network administration into cloud infrastructure, security, and increasingly, technology leadership. Rather than following a traditional leadership track, he built his experience by staying close to technology and gradually expanding the scope of the problems he was responsible for solving.

His interest in cybersecurity began while working at Consigli Construction, where he worked with the operations team and gained exposure to areas such as endpoint detection, logging technologies, and messaging security. It was an opportunity to understand how security fit within the broader infrastructure environment and became an area he continued to pursue.

That experience became particularly valuable when Eric joined Akoya Biosciences, where he helped strengthen the security program as the company continued to grow. His responsibilities expanded across security tooling, incident response, and longer term program development, giving him hands on experience with the different stages of building a more mature security environment.

As the program evolved, Eric helped expand its capabilities and bring in additional resources, including support for around the clock security operations. With a stronger foundation in place and a dedicated security engineer eventually taking greater ownership, Eric shifted his focus more heavily toward infrastructure.

The experience gave him a valuable perspective on how security and infrastructure intersect, something that continues to influence his approach today.

BRINGING SECURITY INTO INFRASTRUCTURE

After a successful tenure at Akoya, Eric joined ElevateBio, where his role has continued to evolve. He initially came into the organization focused on cloud operations before expanding his responsibilities across a broader infrastructure program.

Today, Eric leads the Infrastructure Operations Center, or IOC. The program spans systems, cloud and network operations, with AI operations becoming an increasingly important part of its scope. Security is integrated throughout each of those areas rather than operating separately from the infrastructure program.

For Eric, his background across both disciplines helps him think beyond which security tools are in place. He is equally interested in how those tools are deployed, how they are configured, and where automation can improve the environment.

That operational mindset has become central to his role. His focus is shifting from personally providing services across each area to creating a program that can operate more efficiently while still meeting the needs of security and other stakeholders.

"I came in as a lead individual contributor and now I'm transitioning toward more leadership," he explains. "My focus has shifted from being the person providing the services toward being more of an enabler."

FROM TECHNICAL EXPERT TO LEADER

As Eric takes on more leadership responsibility, some of the most valuable lessons have come from an unexpected place: his earliest days working on a help desk.

Infrastructure roles can naturally become centered around projects and technology. Leadership has required Eric to shift more of his attention toward understanding the business and building relationships with the people his program supports.

"I actually draw on a lot of experience from just being a

help desk person" he shares. "In those roles, you're forced to connect with people first and have that customer service mentality. You understand their needs more than just the technologies you're providing them."

He continues, "I came up through the classic help desk, sysadmin, network admin, infrastructure approach. Now I'm trying to deputize and promote technical authorities from within my program and facilitate those relationships."

THE RAPID RISE OF AI OPERATIONS

Eric's priorities have changed quickly since joining Elevate. His first year was heavily focused on cloud, including how the organization could govern its environment while continuing to scale securely. The following year brought a greater emphasis on network operations and improving how the organization worked with its service providers.

Then AI operations entered the conversation.

Eric sees an opportunity for AI to remove some of the limitations that slow people down. Rather than requiring IT to solve every challenge directly, employees can increasingly use AI tools to address certain needs themselves. That has opened new possibilities for the business while creating a different challenge for technology leaders tasked with understanding how those tools are being used.

For Eric, there is no perfect playbook. The technology is moving too quickly, and organizations are developing their approaches in real time. His response has been to identify the people within the business who are already engaging with AI and strengthen those relationships so his team can better understand emerging use cases.

OPTING OUT VS. OPTING IN

As AI adoption grows, Eric believes technology leaders need to understand what employees are trying to accomplish before drawing conclusions.

"One approach that has been great is leading with listening," he explains. "What are you doing? How are you trying to do it? What can I learn from what you're doing as the user?"

The speed of AI makes that approach even more important. New capabilities are reaching employees before many IT or governance teams have an opportunity to fully evaluate them.

"2026 is the era of opt out. It's no longer about opting in," Eric observes. "Across the industry, new capabilities are reaching people faster than governance teams can evaluate them. That's why staying close to how people work matters so much. It helps keep the technology from getting ahead of the conversation."

For Eric, keeping pace begins with visibility and communication. By staying close to employees who are experimenting with the technology, his team can better understand what is happening across the business and determine where IT can help enable those use cases responsibly.

CONNECTING TECHNOLOGY TO BUSINESS

That same emphasis on understanding people extends beyond AI. As Eric's role becomes more strategic, he is increasingly focused on ensuring the teams and providers he works with understand why their work matters.

Rather than treating infrastructure projects as isolated technical initiatives, he tries to connect decisions back to a corporate goal or IT objective. That context helps teams understand the outcome they are working toward instead of just completing an individual task.

One of the more difficult parts of that responsibility is bringing together providers that naturally operate within different specialties. Eric describes the challenge as "blending context," ensuring that each partner understands how its work connects with other areas and with the broader needs of the business.

His role has increasingly become one of facilitating those connections rather than sitting at the center of every interaction. It is a change Eric has found particularly rewarding because it allows the program to scale while giving others greater ownership.

CONTINUING TO LEARN

Eric approaches his own career development with the same emphasis on relationships. He credits mentors, colleagues, and service providers with helping him grow, but much of that learning begins with curiosity and a willingness to ask questions.

"It is important to always listen, learn, and be curious about what other people are doing, how they're doing it and how they're thinking about things," he shares. "That has been very unlocking for me."

He encourages others to treat the connections they make at industry events as relationships they can actually use. When a new challenge arises, Eric regularly reaches out to people in his network to understand how they are approaching the same problem.

"Don't be afraid to actually use your network," he advises. "When you encounter issues or have interesting puzzles to solve, ping some of those people. What are you doing? How are you thinking about this stuff?"

Long term, Eric sees those experiences leading toward a CTO role. His interest extends beyond infrastructure into how technology and products are designed to solve specific problems, something he describes as a longstanding fascination.

"I am still figuring out the pathway to get there," he shares, "but that has been my North Star."

For Eric, that path continues to take shape as his role expands from technical execution toward leadership. Whether he is building an infrastructure program, navigating the rapid adoption of AI, or developing stronger connections across the business, he continues to grow by remaining close to both the technology and the people it is designed to support.

PROFILES IN *Confidence*

KAMAL SHAH

CEO and CO-FOUNDER
Prophet Security

Headquarters: Palo Alto, CA

Employees: 83

Annual Revenue: Privately Held Company

Kamal Shah's interest in cybersecurity began in 2011 when one of his first startups was acquired by Symantec. After spending a year with Symantec, he joined Sequoia Capital as an entrepreneur in residence, where conversations with CIOs gave him an early view into the security challenges emerging as businesses moved more of their data to the cloud.

Those conversations led Kamal to join Skyhigh Networks as its eighth employee, helping scale the company before its acquisition by McAfee. He later became CEO of a container and Kubernetes security company that was acquired by Red Hat.

Across those experiences, Kamal continued to hear the same frustration from security teams: too many alerts and too many false positives. When generative AI began demonstrating what was possible, he saw an opportunity to approach a longstanding security operations challenge differently.

"The number one complaint I used to hear from our customers was too many alerts, too many false positives," Kamal recalls. "I asked myself: could we leverage AI and agentic AI specifically to automate the process of triaging, investigating, and responding to alerts?"

That question became the foundation for Prophet Security.

SOLVING A PERSISTENT SECURITY CHALLENGE

Before building the company, Kamal and his co-founders went directly to the security leaders experiencing the problem. They spoke with 78 CISOs and security leaders to understand whether existing SOAR technology had successfully addressed alert fatigue.

Only two of those 78 leaders said they were happy with their SOAR implementation. Many had automated only a small number of playbooks and found the process required significant engineering resources to maintain. For Kamal, it validated the need for a different approach.

Prophet Security was founded in September 2023 around the idea that agentic AI could take on more of the investigative work traditionally handled by security analysts. As competition in the market has grown, Kamal believes differentiation starts with something relatively simple: trust.

"Security has been pitched a lot of promises around machine learning and AI over the past several years," he explains. "The approach we took from day one is: how do we make sure that we build trust with our customers every single day?"

For Prophet, that means prioritizing the accuracy of its investigations while giving security teams visibility into how the technology reaches its conclusions. The platform shows the questions it asks, the information it retrieves, and the evidence behind its reasoning. Kamal believes that transparency is essential for security teams being asked to place greater responsibility in the hands of AI.

BUILDING A PLATFORM FOR SECURITY OPERATIONS

Prophet initially entered the market with its AI SOC Analyst, designed to support level one and level two security operations by investigating and responding to alerts. The company has since expanded its vision beyond the initial use case.

In December 2025, Prophet launched AI Threat Hunter, which allows security teams to conduct threat hunts using natural language while also proactively identifying emerging threats. More recently, the company introduced AI Detection

Engineer, extending the platform into another critical part of security operations.

The idea for Detection Engineer came directly from a Fortune 50 financial services customer. The CISO raised a fundamental question: How could the organization prove it had the right detections in place across its attack surface?

Prophet built the product to help answer that question. AI Detection Engineer maps an organization's detections and investigations to the MITRE ATT&CK framework, identifies potential coverage gaps, and helps teams create or improve detections. Early customer conversations have reinforced for Kamal how pressing that challenge has become.

"We are finding that in most cases, customers are missing detections, or they may have a detection in place, but it's not firing," Kamal explains. "Being able to surface those gaps has been eye opening for our customers."

Together, the products reflect Prophet's broader goal of building a platform that supports security operations across multiple roles rather than solving a single workflow. The company also offers a 24/7/365 human in the loop service for organizations that want the advantages of AI while maintaining human oversight around the clock.

LISTENING TO THE CUSTOMER

Customer feedback has played a significant role in how Prophet develops its technology. It began before the company was founded with the conversations Kamal and his co-founders had with those 78 security leaders and continues through the way the company works with customers today.

Each customer is assigned a customer success professional with previous security operations experience. Those conversations are used to understand desired outcomes and identify where the product needs to evolve. Prophet also reserves 20 percent of its engineering capacity for customer requests, with a goal of responding to those requests within 30 days.

That direct connection extends beyond the customer success team. Kamal wants product managers and engineers to speak directly with customers rather than relying on information to move through several layers before reaching the people actually building the technology.

"This is the age of AI. You can't take the traditional approach of a customer communicating with a sales engineer, who then talks to a product manager, who then talks to an engineer," he explains. "We want engineers involved in conversations with customers directly."

For Kamal, that responsiveness is not only part of the customer experience. It influences how quickly Prophet can learn and continue developing its platform.

BUILDING FOR THE AGE OF AI

That same sense of urgency shapes how Kamal thinks about building the company itself. Prophet is growing quickly, and he does not believe the traditional approach to scaling a software company necessarily applies in an AI driven market.

Hiring starts with understanding the problems customers are trying to solve. In customer facing roles, Prophet looks for people with security operations experience who can understand those challenges firsthand. Kamal also values people who are willing to act quickly and remain open to changing how they work as the company evolves.

"The way you build a company in the age of AI is different than the way you have traditionally scaled companies," Kamal comments. "You have to do things differently, otherwise you're not going to scale."

That philosophy extends to how Prophet takes its technology to market. The company is channel first, and sales conversations are always product focused. Rather than spending most of an initial meeting presenting slides, the team moves quickly into the product and demonstrates what it can do within a customer's environment.

For Kamal, showing value is more effective than spending time explaining a problem security leaders already know they have.

STAYING CLOSE WHILE SCALING

As CEO, one of Kamal's challenges is maintaining the customer connection that helped shape Prophet, while building an organization that no longer depends on its founders for every conversation.

In the company's earlier stages, Kamal and his co-founders regularly participated in multiple customer calls each day. As Prophet has grown, more of his attention has shifted toward enabling the broader team to carry those conversations forward. The company conducts training with its sales engineering team every two weeks to keep pace with new features and capabilities.

Kamal still makes a point of joining customer and prospect meetings himself. He believes staying connected to the market is particularly important when both technology and customer expectations are changing.

"The market's moving very quickly, AI is moving very quickly, and we have to be on top of it to make sure that we are also moving quickly," he explains.

That connection between listening and moving rapidly has been consistent throughout Kamal's career. Today, customer feedback continues to influence where the company goes next. "We are just getting started," he shares.

KYLE BUBP

CISO
Avid

Headquarters: Burlington, MA

Employees: 1,400

Annual Revenue: Privately Held Company

PROFILES IN *Confidence*

Kyle Bubp's interest in technology started early. Growing up in the 1990s, he was introduced to computers by his father, who built and repaired them as a side business. By seven or eight years old, Kyle was already exploring MS DOS, bulletin board systems, and the early internet.

Kyle's first significant exposure to cybersecurity came while supporting a Department of Defense contractor. At the time, security was not a separate function. IT administrators were responsible for maintaining systems while also conducting vulnerability scans, patching, and hardening configurations to meet strict government requirements.

"Even though I didn't have security in my title, that first job contracting with the Department of Defense taught me so much about good hygiene and good security," Kyle recalls.

Those fundamentals would remain important as his career expanded from hands-on technical work into consulting, entrepreneurship, security architecture, and eventually executive leadership.

SEEING SECURITY DIFFERENTLY

One of the most influential periods in Kyle's career came while leading a security practice for a technology reseller. Working directly with customers gave him visibility into security programs across many different organizations, and he began noticing a common problem.

Companies were continually investing in new security technologies, but another product was rarely what they actually needed. "They're not one tool away from becoming more secure," Kyle explains. "They lacked a strategy and they lacked the ability to measure their program. They had shelfware, meaning they had bought products that they never implemented or didn't fully implement."

The experience eventually led Kyle and a colleague to launch Savage Security, where they helped organizations assess their programs and improve security without simply defaulting to adding more technology. The company was eventually acquired, continuing a career path that would take Kyle to work at AWS and later JLL.

At JLL, Kyle became Executive Director of Attack Surface Management, with responsibility across security architecture, vulnerability management, cloud security, and application security within a global organization of more than 100,000 employees.

By then, he knew that the natural progression of his career path would lead to CISO.

FINDING THE RIGHT OPPORTUNITY

When Kyle saw that Avid was looking for a CISO, the opportunity immediately stood out for both professional and personal reasons. A longtime musician, Kyle had played guitar since his teenage years and was already familiar with Avid through Pro Tools, which he had used for recording and editing audio.

"I thought it would be really cool to work for a company where, on the side of my personal life, I use their software," he recalls.

Today as CISO, his responsibilities extend beyond a traditional security organization. In addition to overseeing the breadth of Avid's cybersecurity program, Kyle is responsible for enterprise IT, including systems and network administration. He believes that combination provides an important advantage.

"Security teams struggle because they actually can't make the changes to make the company more secure," Kyle explains. "They're simply advising on the risk and recommending the remediation, but they're wholly reliant on

other teams to execute." Having both teams aligned under one structure, he believes, can accelerate risk reduction.

GETTING BACK TO THE FUNDAMENTALS

That ability to execute is particularly important given Kyle's priorities for the next several years. Rather than looking for another security product to add to his portfolio, he is focused on maximizing the technologies Avid already owns and addressing more systemic issues within the environment.

"We're not one tool away from making Avid more secure," he says. "I've largely applied all the bandaids we can apply. Now I want to go after the systemic issues."

For Kyle, that means improving configuration management, strengthening processes, and hardening environments against known configuration standards. It is work that may not generate the same excitement as buying a new technology, but he believes it can have a greater impact on security.

He compares the approach to personal health. Much like jumping on the latest fad diet, purchasing another security product can be relatively easy. Consistently maintaining strong configurations and processes requires considerably more discipline, much like consistently maintaining a healthy diet and exercise program. "There are a lot of things that don't require a tool," Kyle explains. "It's just human work that has to be done."

FINDING PRACTICAL VALUE IN AI

Kyle brings a similar perspective to artificial intelligence. He sees significant opportunities for AI to augment his team, particularly when it can eliminate repetitive work and give employees more time to focus on improving the security program.

One example is customer security questionnaires. Rather than purchase another SaaS platform, Kyle challenged a team member to explore whether they could build something themselves. Within roughly a day, they developed an internal AI powered tool that can process questionnaires and produce responses for human review in minutes.

Avid is also using AI within email security, where automation has replaced a previously manual review process and is saving the security team significant time each week.

Those use cases have made Kyle optimistic about AI as an efficiency tool, but he remains measured about some of the broader predictions surrounding its impact on cybersecurity. "I don't know that we really understand what the actual ROI of AI is quite yet," he says.

SECURITY FUNDAMENTALS IN AN AI WORLD

Kyle has heard predictions that AI will dramatically increase the scale and sophistication of cyberattacks. While he expects AI to make certain capabilities more accessible to attackers, he does not believe it changes the fundamental problem defenders need to solve.

"At the end of the day, they still have to exploit vulnerabilities, the same misconfigurations, trick the same humans" Kyle explains. "If we maintain some of the base principles of security, like principle of least privilege, good configuration management, understanding our asset inventory, and controlling what happens on those assets, I think we'll be okay."

His greater concern is making sure organizations do not become distracted by AI hype at the expense of those fundamentals. "I'm not afraid of the machine," he says. "I'm afraid of how much money we're spending with AI in hopes that we see an ROI one day."

CHANGING THE CULTURE OF SECURITY

Kyle expects his team to identify problems and take initiative rather than wait for direction. He also does not want to be the only person identifying risk or developing solutions. "If I am the smartest person on the team, that's a problem, because I can't be the one solutioning for everything," he explains.

The role of the security team, he believes, should be that of a risk advisor. If someone wants to purchase a technology or pursue building a new feature or solution, Kyle's team evaluates it and explains the potential risk. The appropriate business leader then decides whether that risk is acceptable.

"We're not gatekeepers," Kyle comments. "If you want to go put your hand on a hot stovetop, we'll tell you all the reasons why you shouldn't do it, but at the end of the day, if you accept the risk, it's on you."

BUILDING TRUST THROUGH TRANSPARENCY

The same philosophy shapes Kyle's relationship with executive leadership and the board. He believes CISOs need to be willing to present the organization's risk as it actually exists, even when the picture is uncomfortable. Trying to make a security program appear stronger than it is ultimately undermines a CISO's responsibility as a risk advisor.

"If I'm hiding that risk to make myself look better, that's a really bad place to be in," Kyle says.

"Everyone has things in their organization that they need to address. Every program has gaps," he explains. "If we're just honest with each other and we're a little vulnerable with each other, I think that helps establish trust."

It is an approach that connects back to the lessons Kyle learned early in his career. Security does not always require another product or a more complicated solution. Often, meaningful progress comes from understanding the risk, addressing the fundamentals, and being willing to do the difficult work required to make the organization stronger.

PROFILES IN *Confidence*

PREMAL "PREM" PATEL

DIRECTOR OF CYBERSECURITY OPERATIONS

ACV Auctions

Headquarters: Buffalo, NY

Employees: 3,200

Annual Revenue: $760 Million

Premal "Prem" Patel's path into cybersecurity began with curiosity. Growing up, he was always interested in understanding how things worked, often taking them apart and finding a way to put them back together. Yet technology was not initially where he imagined building his career.

Prem entered college on a medical pathway with plans to become a doctor. During his second year, he reconsidered that direction and turned toward an interest that felt more natural. He added computer science alongside biology for his undergraduate studies and later earned a master's degree in cybersecurity.

"I'd rather be tinkering, breaking things, and hacking things," he recalls of discovering cybersecurity as a career path.

Prem began gaining professional experience while still in school through a co-op at MIT Lincoln Laboratory, where he had the opportunity to work with the Department of Defense. The experience introduced him to the structure and discipline of cybersecurity within government and helped establish the technical foundation that would shape his career.

From there, he moved into consulting with Deloitte and Ernst & Young. Working across industries including healthcare, financial services, automotive, oil and gas, and aviation gave Prem exposure to organizations with very different priorities and risk environments. It also taught him to think about cybersecurity through the lens of the business it protects.

BUILDING THE NEXT STAGE AT ACV

In 2026 Prem joined ACV Auctions as Director of Cybersecurity Operations. His initial conversations with the CISO and the broader team immediately stood out.

ACV presented the kind of challenge that aligned with his experience. The organization had evolved from its startup roots following its IPO, creating an opportunity to continue maturing the security capabilities alongside the business.

Prem saw a chance to bring together lessons from his consulting and industry experience to help evolve cybersecurity operations into a more mature function. His vision includes growing a team that began with only a few people into a globally supported operation capable of providing coverage around the clock.

His responsibilities extend across incident response, security operations and threat detection and response, while also touching areas including identity and access management, third party risk management and security awareness. As AI becomes increasingly embedded within the business, AI security has emerged as another important area of focus.

CREATING THE FOUNDATION FOR AI SECURITY

Prem views AI as a double-edged sword, where its ability to improve productivity is significant, but the same technology is also accelerating risk.

For security leaders, he believes two areas have become particularly important: data and identity. Organizations need visibility into where data resides, where it moves, and who or what can access it. That last distinction is increasingly important as nonhuman identities and AI agents begin operating at a scale traditional identity programs were not necessarily designed to address.

At ACV, AI is beginning to influence both development and products, making those foundational controls increasingly important. Prem believes the broader security mindset must evolve with it.

"We went from security as reactive to proactive to now zero trust and assumed breach," he explains. AI can accelerate the exploitation of vulnerabilities from days or weeks to

hours or minutes, requiring organizations to rethink how quickly their defensive capabilities can respond.

That does not mean Prem believes organizations should slow innovation. Instead, he sees security's responsibility as helping the business adopt AI responsibly while understanding its risks. "We don't want to be a roadblock or a gatekeeper," he says. "It's more of the fact that we want to create guardrails for the path forward."

Those guardrails also need to demonstrate business value. As organizations invest heavily in AI, Prem believes security leaders will increasingly need to communicate whether those investments are delivering meaningful returns while ensuring the technology is being implemented with a safe, secure, and compliant perspective.

GOING DOWN THE RABBIT HOLE

Keeping pace with AI requires more than following headlines. Prem has adopted advice from one of his mentors to choose a topic and go deeply into it until he holistically understands how the technology works.

For AI, that has meant studying technologies such as Model Context Protocol and APIs rather than limiting his focus to their security implications. Prem wants to understand the underlying technology first, then translate that understanding into practical controls. "The biggest piece is, how do you take that theoretical aspect and then operationalize it?" he says.

That question becomes increasingly significant as organizations introduce AI agents capable of interacting with sensitive systems and information. Prem believes access needs clear checks and balances, particularly when agents are connected to environments such as email or corporate data. Human oversight remains an important part of that model.

"There always has to be some sort of human in the loop to make sure that there is a certain level of checks and balances for that agent," he explains.

TRANSLATING SECURITY INTO BUSINESS VALUE

Prem's consulting background has also influenced how he communicates cybersecurity. Working across industries taught him that the technical risk may change, but the most important question remains consistent: who is ultimately impacted?

Prem says that for healthcare organizations, that might mean protecting patients and their sensitive information. In another industry, the priority may look entirely different. Understanding that context allows him to connect cybersecurity decisions to what matters most to the organization and its customers.

That perspective shapes how he communicates with both technical and nontechnical audiences. "It's an art of doing the technical to nontechnical," Prem explains. "Keep it simple to the point where they can understand it as well. Because we can communicate as much as we want, but if they don't understand it, then what's the point?"

For Prem, effective communication begins by understanding the other person's perspective rather than expecting them to adopt the language of cybersecurity. That ability has become important as security moves closer to business strategy and leaders are asked to explain emerging risks such as AI to audiences across the organization.

LEARNING THROUGH LEADERSHIP

Prem approaches leadership with the same curiosity that initially drew him toward cybersecurity. While becoming a CISO or moving into another senior technology leadership role is a long-term goal, he is focused on continuing to learn before getting there.

"I value the failures much more than the successes because that's how you grow as a leader," he says. "That's how you grow as a person as well."

Much of that growth comes from the people Prem has intentionally surrounded himself with. In addition to formal leadership training and independent learning, he has developed a network of mentors he can turn to when working through difficult decisions. His core group of mentors spans leaders with experience running large organizations, building businesses, and creating cybersecurity companies.

Prem encourages emerging cybersecurity professionals to build those relationships by being willing to make the first move. "The answer will always be 'no' if you don't ask," he says. "You must put your foot forward to be able to say, 'Hey, I genuinely want to learn.'"

That willingness to keep learning is particularly important as cybersecurity enters another period of rapid change. Prem believes the industry is still determining what mature AI security will ultimately look like. Organizations are experimenting, learning where gaps exist and beginning to establish more consistent controls. He expects greater standardization to emerge as the technology and security practices surrounding it mature.

For Prem, navigating that uncertainty comes back to the same approach that has shaped his career: understand the technology deeply, connect security to the people and business it protects, and remain willing to learn as the landscape changes.

PROFILES IN *Confidence*

RAJ SHARMA

HEAD OF INFORMATION SECURITY
Northern Bank

Headquarters: Woburn, MA

Employees: 300

Annual Revenue: Privately Held Company

Raj Sharma began his career in cybersecurity more than 20 years ago, when the field was still commonly referred to as data security. Fresh out of college and working as a management trainee at a bank, Raj was approached by the CTO about an opening for a data security administrator.

"At the time, I had not known anything about data security. It was very new, but I decided to give it a shot," Raj recalls.

That opportunity introduced him to what he describes as the other side of technology and set the direction for his career. Over the years, Raj has watched cybersecurity evolve through the shift from on prem environments to the cloud, the rise of ransomware, and now the opportunities and risks created by AI.

Raj spent 16 years at Eastern Bank, progressing from Data Security Administrator to pivotal leadership positions within the cybersecurity program. Along the way, he played a key role in developing and maturing the organization's information security function.

MATURING SECURITY THROUGH PARTNERSHIP

In 2018, Raj joined Northern Bank with an opportunity to continue to mature its information security program. Today, his responsibilities span all aspects of cybersecurity, giving him visibility into each program area. However, some of the most important work he has done has been around relationships.

Coming from a much larger organization, Raj recognized the importance of working closely with Northern Bank's IT team and business leaders. Rather than positioning security as a separate function, he wanted the organization to see him as a partner who could support innovation and growth while ensuring the appropriate guardrails were in place.

That philosophy has become central to how Raj views the role of a security leader. "A CISO really must have a good understanding of the business, a good understanding of the business objective, and a good understanding of the business strategy," he explains.

Getting involved early is critical. When security understands where business leaders are heading and what technologies they want to use, it helps build security into the process rather than evaluating risk after decisions have already been made.

LEARNING TO SPEAK THE LANGUAGE OF BUSINESS

Raj learned the importance of business communication through experience. Earlier in his career, he remembers presenting a technology solution to senior leadership and walking away believing he had done a great job. Afterward, one of the executives approached him with candid feedback that despite the work Raj had put into the presentation, he had not explained what leadership really needed to know.

"What's going to be the value to the business? What's going to be the cost? And if there's risk, put those risks in business terms so that it's easy to understand," Raj recalls being told.

It was an awakening moment. Technical expertise might help a security leader identify risk, but communicating that risk requires understanding what matters to the audience.

Today, Raj thinks about security conversations in terms of areas such as business objectives, cost, potential loss, and organizational impact. He encourages other security leaders to do the same, particularly when communicating with executives and boards.

PREPARING FOR WHAT COMES NEXT

Raj's priorities reflect how quickly the security landscape continues to evolve. Resilience and governance remain foundational, but he is also focused on AI governance, phishing resistant multifactor authentication, post quantum

preparation, and security awareness.

Some of those risks may still be years away, but Raj believes organizations should begin preparing before they become immediate problems. With post quantum security, for example, that means understanding where certificates and encryption are used today and considering how those technologies may eventually need to change.

At the same time, employees remain a critical part of the equation. “Our employees are our biggest control when it comes to security,” Raj explains.

AI is making that responsibility more complicated as fraudulent emails become increasingly difficult to distinguish from legitimate communications. For Raj, continuing to strengthen security awareness is therefore just as important as investing in emerging technologies.

CREATING STRUCTURE AROUND AI

AI governance has become one of Raj’s most immediate priorities as Northern Bank navigates adoption from multiple directions.

Existing vendors are increasingly adding AI capabilities to their products, while employees and business teams are interested in platforms such as Copilot and other large language models. Raj believes both require oversight.

The organization needs to understand how vendors have secured their AI capabilities and whether new functionality meets Northern Bank’s standards. Internally, it also warrants visibility into which AI tools are being used and how employees interact with them.

“There must be good governance around AI,” Raj says. “Making sure that this process is vetted and making sure that we have good control over what AI tools are being used.”

Northern Bank has established a governance committee where these questions may be evaluated as the technology continues to evolve. For Raj, the goal is not to prevent adoption, but to create a process that allows the business to take advantage of AI within appropriate boundaries.

DOING MORE WITH A LEAN TEAM

Like many security leaders, Raj faces the challenge of managing increasingly complex risks with finite resources. “How can we sustain these big challenges while remaining a lean shop?” he asks. “I have a small team, but we have these big challenges.”

That reality makes prioritization especially important. It also reinforces why Raj wants security integrated into business decisions. When leaders understand risk before making a decision, the organization can make more informed choices about where resources will have the greatest impact.

Raj brings a collaborative approach to leading his own team. He wants employees to take ownership with their own ideas and have the support they need to succeed. “I consider myself to be more of a transparent, collaborative leader,” he shares. “I allow my team members to feel empowered to take ownership and for me to be by their side in case there are any issues.”

With a field that changes as quickly as cybersecurity, he also places significant emphasis on continued learning. For Raj, training matters more than simply accumulating certifications. He looks for people who are curious and willing to continually develop their skills.

MAKING YOURSELF VISIBLE

Raj holds himself to that same expectation for growth. He attends and speaks at conferences, participates in panels, maintains relationships with peers, and regularly seeks feedback from colleagues and other leaders about his own strengths and weaknesses.

Building those relationships did not always come naturally. “At the beginning of my career, I was more of an introvert,” Raj recalls. Over time, he realized that approach meant people often came to him only when there was a security problem. To become a stronger leader and business partner, he needed to make himself more visible.

Today, Raj encourages other cybersecurity professionals to do the same, even if they start small. An email or LinkedIn message can be the first step toward developing a relationship with someone they respect.

He also gives back through the Massachusetts Cyber Exchange, where he mentors college students preparing to enter the field. For Raj, mentorship reflects a broader evolution within cybersecurity itself.

“Security is no longer this person who’s sitting in the corner by themselves,” he says. “A security professional needs to be in alignment with the business lines, with their peers.”

It is a lesson that mirrors Raj’s own career. As cybersecurity has evolved from data security into a strategic business discipline, he has evolved with it, continually learning, strengthening relationships, and ensuring security remains connected to where the business is going next.

PROFILES IN *Confidence*

SALAAM HARRIS

CISO, CRICO/Risk Management

The Risk Management Foundation of the Harvard Medical Institutions

Headquarters: Boston, MA

Employees: 200

Annual Revenue: Privately Held Company

Salaam Harris's interest in technology started long before it became his career. As a child, he was fascinated by understanding how things worked, taking apart electronics, experimenting with circuit boards, and tinkering with his first computer.

His professional path began in the U.S. Air Force, although not initially in technology. Salaam started as a fighter jet mechanic before an opportunity emerged to retrain in cyber operations supporting a reconnaissance intelligence unit. The transition allowed him to combine his longstanding interest in technology with the discipline and mission focused environment of the military.

From there, Salaam continued developing his technical expertise through training and education while taking on roles with Raytheon and Northrop Grumman. At Northrop Grumman, his work included helping to secure training environments and simulators for the Navy. He later moved to South Shore Health, where he helped mature the cybersecurity program and build out its security operations capabilities.

Those experiences eventually led Salaam to Dragonfly Therapeutics, where he was the first dedicated cybersecurity professional and had the opportunity to build a program from the ground up. It was an experience that prepared him well for the CISO role he holds today.

BUILDING WITH THE MISSION IN MIND

When the opportunity arose for Salaam to step into a CISO position, the ability to shape a cybersecurity program around the needs of the organization appealed to him.

"I like a challenge," Salaam shares. "I like to make sure that I have the opportunity to develop a program and influence that program from the ground up, from strategy and governance to operations, resilience, and specifically the culture."

It is an approach heavily influenced by his military background. As Salaam advanced through the Air Force, he was given significant responsibility early in his career. Managing large budgets and working around multimillion dollar aircrafts taught him to consider how individual decisions could affect a much larger mission.

That perspective translates directly to cybersecurity. For Salaam, a security strategy cannot exist independently from the organization it protects. Priorities and investments need to connect back to what the business is ultimately trying to accomplish.

The same is true for culture. Technology and processes can only go so far if employees do not understand why security matters. Salaam focuses on making cybersecurity relevant to people by connecting their individual actions to consequences they can understand.

Once employees understand that connection, Salaam sees them as an extension of the security team. He even has a name for them, calling them "cyber warriors."

TURNING CYBER RISK INTO BUSINESS DECISIONS

Today, Salaam's responsibilities span the overall cybersecurity strategy and risk posture of the organization. But he views communicating that risk to executives and board members as an equally important part of the CISO role.

The goal is not to just report vulnerabilities or threats. It is to provide leadership with enough context to make informed decisions about the organization.

"A big part of my role is translating that information and that

risk posture to our executive leadership team and our board members," Salaam explains. "More importantly, it is making sure that they have the appropriate information to make those decisions."

That requires participation across the organization. Salaam believes the effectiveness of a cybersecurity program ultimately comes back to whether people understand what the security team is doing, why it matters, and how they can contribute.

PREPARING FOR AI RATHER THAN WAITING

As cybersecurity priorities evolve, Salaam sees AI governance and security as one of the most pressing issues facing CISOs. Identity is particularly important as AI agents introduce an entirely new category of nonhuman identities into enterprise environments.

"We have to be thinking about them as another employee," he explains. Security leaders need to consider what level of access an AI agent has and what actions it can take on behalf of the organization.

Salaam does not believe the answer is to wait until the AI landscape becomes clearer. Organizations that take that approach risk falling behind. "If you're not using AI in this day and age, you're going to be left behind," he says. "You've got to have guardrails, controls, policies, and governance in place, but you also have to make sure that you're agile and can adjust and shift because this space is moving extremely quickly."

For Salaam, security should enable that adoption rather than stand in its way. The objective is to help the business use AI while creating enough structure to manage the risks that come with it.

RETHINKING IDENTITY

AI is also amplifying an identity challenge that was already becoming more complicated. Traditional environments were relatively contained, with identities and infrastructure largely residing on premises. Today, SaaS applications, cloud environments, and now AI agents have expanded where identities exist and what they are capable of doing.

"Identities are everywhere," Salaam explains. "You have to make sure that you know where all these identities are."

That begins with visibility and a comprehensive inventory, but it also requires understanding what those identities are actually doing. Salaam believes organizations need insight into whether an identity is actively performing tasks, what it can access, and whether accounts remain in the environment that should no longer be there.

As AI agents become more autonomous, that visibility will become even more important. Organizations are no longer governing access exclusively for employees. They are increasingly responsible for understanding the permissions and activities of machines acting on their behalf.

WHY PEOPLE STILL MATTER

Even as AI becomes more capable, Salaam pushes back on the assumption that it will immediately reduce the need for cybersecurity professionals.

Security organizations already face limited resources while technology costs continue to increase. At the same time, security stacks are becoming larger and more complex, creating additional technologies that need to be implemented and operationalized.

AI adds another layer because organizations need people who can analyze what AI produces and oversee what agents are doing. When asked where he would invest if resources were unlimited, Salaam did not hesitate.

"It would 100% go towards people," he shares. "You can go buy more technology, but who's going to manage that technology? There is a balance to it, but you're always going to need more people than technology."

In fact, Salaam believes the near term effect of AI could be the opposite of what some organizations expect. Rather than immediately reducing cybersecurity staffing needs, the speed of AI adoption and the complexity of governing it may require more resources as organizations learn how to manage the technology effectively.

PUTTING PEOPLE FIRST

Salaam describes his leadership style as a blend of servant and transformational leadership, an approach shaped considerably by his military career and the leadership training he received throughout his years in the Air Force.

At its center is a straightforward principle that people come first. Transparency is also very important to him. Salaam wants team members to feel comfortable telling him when something is not working or even when they disagree with him.

"That psychological safety is extremely important within cybersecurity," he explains. "I need people to be comfortable and willing to let me know if something isn't working. We can always make adjustments, but if you don't tell me, I won't know."

That philosophy extends beyond his own team. Salaam regularly mentors people outside his organization. For him, giving that time back is a reflection of the support he received throughout his own career. "I wouldn't be where I am right now without the people that helped me get to where I am," he shares. "So I make sure that I always try to give that back to the community."

Across his career, the environments have changed considerably, from military intelligence and defense to healthcare and corporate cybersecurity. But the principles Salaam brings to each challenge have remained consistent. He is always focused on understanding the mission, building a culture where people understand their role in protecting it, and never losing sight of the people behind the technology.

PROFILES IN *Confidence*

SEAN CALISTA

SR. DIRECTOR OF INFORMATION TECHNOLOGY AND SECURITY

CloudZero

Headquarters: Boston, MA

Employees: 150

Annual Revenue: Privately Held Company

Sean Calista discovered information security earlier than most. Before graduating from high school, he was already working at a cybersecurity company, writing detection signatures and gaining firsthand experience with security technologies.

He went on to study information security and network engineering at Rochester Institute of Technology, followed by a co-op and eventual role at MIT Lincoln Laboratory. Working within a federally funded research environment focused on national defense broadened his cybersecurity experience, but Sean ultimately found himself drawn back to the fast-paced startup environments where he had started his career.

That decision set the direction for what came next. Over the next two decades, Sean would build his career across security engineering, incident response, infrastructure, and leadership, often joining growing organizations where he had the opportunity to build and mature security programs.

BUILDING SECURITY FROM THE GROUND UP

Sean joined athenahealth in 2013 as one of the company's early security hires, where his responsibilities included incident response, security engineering, and implementing controls to protect sensitive customer information. He later moved to LogMeIn, initially building security capabilities across the organization's global corporate environment before shifting toward infrastructure security for its production systems.

It was during this period that Sean learned one of the lessons that continues to influence his approach today: the strongest security control is not necessarily the most restrictive one.

Working alongside his boss and mentor, Sean gained valuable skills including the important balance of integrating business objectives and security risk.

The experience helped Sean understand that security leaders must find the controls that are appropriate for their organization and its risk appetite rather than pursuing security in isolation.

That philosophy followed him through roles at Drift, TrueMotion, and Relay Therapeutics, where he repeatedly found himself joining organizations with little or relatively small security functions and helping build them into mature programs. At TrueMotion, he established the security incident response team and information security committee while developing the metrics and objectives needed to connect security strategy with business priorities. At Relay Therapeutics, he again helped establish the security program, including its framework, budget and objectives.

Building has become what Sean describes as his "bread and butter." Today, he brings that experience to CloudZero, where he serves as Senior Director of Information Technology and Security and has spent the past several years building out the company's security program.

BUILDING TEAMS AROUND YOUR WEAKNESSES

As Sean has transitioned from technical practitioner to security leader, he has also learned that leadership does not require being the strongest person in every discipline.

His background is rooted heavily in incident response, infrastructure, and security engineering. When building the team at CloudZero, he deliberately looked beyond those strengths.

"I always have the mentality of focusing on, and augmenting, your weaknesses," he explains.

Rather than hiring first in the areas he knew best, Sean prioritized expertise in areas where others could bring deeper knowledge. His first information security hire focused on application security, while another was brought in to lead governance, risk and compliance.

For Sean, surrounding himself with people who can bring greater depth to specific areas creates a stronger security organization while also allowing those individuals to grow as leaders themselves.

It reflects a larger lesson he has learned throughout his career: growth comes from recognizing what you do not know and surrounding yourself with people who can make you better.

LEARNING TO THINK LIKE THE BUSINESS

Sean's technical background is extensive, but his approach to security is equally grounded in business. Some of that perspective came from his upbringing. His father and grandfather worked in sales and business roles, exposing Sean to a different way of thinking than the engineering environment in which he ultimately built his career. But he credits much of his development to learning on the job and, in particular, learning from mentors.

Three people have had an especially significant influence: Chris Harrington, who gave Sean his first opportunity in the security industry at Nitro Security and later hired him at MIT Lincoln Laboratory; Gabor Tokaji when he was at LogMeIn & TrueMotion; and CloudZero founder Erik Peterson.

Sean believes aspiring leaders should seek out people who have already reached the level they hope to achieve. That philosophy has influenced how Sean evaluates his own career opportunities. The organization matters, but he believes the person you work for can have an even greater impact on your development.

"The most important thing is who your boss is," Sean says.

At CloudZero, working for Peterson has helped Sean continue evolving from a technical security leader into a broader business executive as he works toward his long-term goal of becoming a CISO.

FINDING THE BALANCE WITH AI

The same balance Sean learned earlier in his career is becoming increasingly important as organizations adopt AI.

CloudZero itself sits directly within that evolution. The company helps organizations understand AI ROI, including how AI spending can be attributed to specific features and customers. As businesses invest significant amounts into AI, understanding whether that spending is delivering value is becoming an important business question.

From Sean's perspective as a security leader, however, AI is also fundamentally changing who can build technology.

In his 20 years in information security, Sean says he cannot remember another point when people outside traditional technical roles could easily develop their own applications. AI has changed that. Finance and HR leaders can now build tools and applications themselves, creating opportunities for innovation while introducing a new set of security considerations.

Sean sees AI agents almost like another workforce that must be governed. They need the right access and the right data, and organizations need to think about how information is made available to them.

The challenge is doing that without undermining the innovation AI makes possible. "How can I keep the business moving fast on AI without sacrificing security? It's a delicate balance." Sean says.

Simply shutting AI down is not a viable strategy in his view. "If you don't adapt with AI, you're going to lose," he says.

Instead, Sean believes organizations must understand the associated risks and establish controls that allow the business to move forward securely.

MAKING IT EASY TO DO THE RIGHT THING

At CloudZero, one way Sean's team is addressing this challenge is by creating what they call a "golden path."

As employees across the organization gain the ability to build applications, security cannot assume everyone will understand the infrastructure and controls required to deploy them safely. Rather than expecting every employee to become a security expert, Sean wants to create an approved path that makes secure deployment easier.

That may mean providing designated cloud environments and incorporating protections such as identity controls so employees can implement applications with AI while limiting risk to the business.

The philosophy behind it is straightforward. "The way to win in this industry is to make it easy and do the right thing," Sean says. "When you make it hard to do the right thing, that's when things never go your way."

That mindset extends beyond technology. Sean also believes security programs cannot scale if responsibility for security remains solely within the security team. CloudZero uses a security champions program to establish advocates throughout the business who can help extend the security team's reach. As AI enables more employees to become builders themselves, those relationships are becoming even more valuable.

GIVING THE NEXT GENERATION A CHANCE

As Sean looks toward becoming a CISO, he is also thinking about the responsibility established leaders have to those entering the profession. His own career began because someone was willing to take a chance on him, a high school student.

Years later, Sean remembers discussing that decision with Chris Harrington, the person who initially hired him. Harrington admitted he had questioned what a high school student could contribute. But he gave Sean the opportunity anyway.

"If he didn't give me that chance, I'm not sure where I would be," Sean says. It is a lesson Sean believes is particularly relevant as AI begins changing the entry level jobs that traditionally helped people establish themselves in cybersecurity.

Security leaders have an opportunity to actively develop the next generation, whether that means creating internships or mentoring someone earlier in their career.

Sean also encourages younger professionals not to wait for those relationships to happen organically. He recommends finding leaders they respect, including people outside cybersecurity, and asking for their time. Even a regular coffee or brief conversation can become an opportunity to develop business acumen and learn from someone who has already navigated certain challenges.

For Sean, that cycle of opportunity is central to leadership. His career began because someone gave him a chance. It grew because mentors challenged him to think differently about security. Now, as AI reshapes both cybersecurity and the paths people take into the profession, he believes today's leaders have a responsibility to provide those same opportunities to others.

"I truly believe that what's good for the person coming up is good for the industry," Sean says, "and it's just good for us as humans to help each other out."

What Leaders Reveal About the Changing Role of Cybersecurity

By Katie Haug

Cybersecurity has spent years trying to get closer to the business. Security leaders have talked about earning a seat at the table, communicating risk more clearly, and moving beyond the perception that security exists primarily to say no.

Across our latest conversations with security and technology leaders, that shift no longer feels aspirational. It is changing how programs are built, how risk is communicated, and how security leaders define success. The most striking takeaway is that leaders are increasingly focused on helping the business move forward, not simply protecting it from risk.

Artificial intelligence is accelerating much of that change. Business teams are moving quickly, experimenting with new tools and looking for ways to use AI to create value. Security leaders know they cannot wait until those decisions are complete and then step in to evaluate risk. They need to be part of the process from the beginning.

But AI is only part of the story. Underneath the technology is a broader shift toward business alignment, disciplined investment, stronger executive communication, and a more practical approach to risk.

SECURITY IS BEING MEASURED BY THE BUSINESS IT ENABLES

For many years, cybersecurity success was often measured through controls, frameworks, vulnerabilities, or the technologies deployed across the environment. Those measures still matter, but several of the leaders we spoke with are defining success more broadly.

Don Baham, Chief Information and Security Officer at Rubicon Founders, believes security needs to connect directly to where the organization is going.

“If I can’t translate what we’re doing from a technology or security standpoint to creating value either for the firm or portfolio company, then I failed,” he explains.

For Don, that means understanding what investment teams and portfolio companies are trying to accomplish and ensuring security priorities support those objectives. He does not want his team pursuing technology simply because it is new. The question is whether the work creates value.

Raj Sharma, Head of Information Security at Northern Bank, takes a similar approach. He believes security leaders need to understand business objectives and strategy well enough to become part of the process rather than a function consulted at the end.

“A CISO really needs to have a good understanding of the business, a good understanding of the business objective, and a good understanding of the business strategy,” Raj explains.

That understanding allows security to support innovation without abandoning its responsibility to manage risk. Instead of starting with, “How do we secure this?” leaders are increasingly asking, “What is the business trying to accomplish, and how can we help them do it securely?”

Sean Calista, Senior Director of Information Technology and Security at CloudZero, is confronting that question directly through AI. He sees employees outside traditional technical roles using AI to create applications and solve problems themselves. His challenge is not determining how to stop that activity, but how to support it responsibly.

“How can I not slow down this AI growth while keeping things somewhat secure?” Sean asks.

The modern security leader is becoming less of a gatekeeper and more of an enabler.

RISK OWNERSHIP IS MOVING BACK TO THE BUSINESS

Another strong theme is how leaders think about risk ownership.

Security has often been placed in the uncomfortable position of approving or denying technologies and projects. Kyle Bubp, CISO at Avid, has deliberately worked to change that perception.

“We are risk advisors and we don’t accept the risk, we don’t hold the risk,” Kyle explains.

When someone approaches his team with a new technology or initiative, security evaluates the risk and communicates

what it finds. The appropriate business leader then decides whether that risk is acceptable.

That distinction matters because it changes accountability. Security is still responsible for understanding risk and providing informed guidance, but it is not the owner of every business decision that contains risk.

Raj sees the same need for shared ownership. One of his challenges is ensuring business leaders understand risk while they are making decisions, which is why he believes information security needs to be involved in the business decision process itself.

This shift also changes the relationship between security and the rest of the organization. When security owns the decision, business teams can begin to view it as the function standing between them and an objective. When the business owns the decision, security can focus on making sure leaders understand the tradeoffs involved. That creates a more collaborative model where the goal is not to eliminate every risk, but to determine which risks make sense in the context of what the organization is trying to accomplish.

It also requires security leaders to become comfortable with a different measure of success. A decision may move forward even when risk remains. The value security provides is ensuring that risk is visible, understood, and considered alongside the potential business value. In that model, a strong security program does not make every decision for the organization. It helps the organization make better decisions for itself.

The role of security is becoming clearer: identify the risk, explain what it means, and provide the business with the information it needs to make an informed decision.

EXECUTIVE INFLUENCE DEPENDS ON TRANSLATION

The leaders who described the strongest executive relationships consistently returned to one skill: translation.

Raj learned this through experience. Earlier in his career, he presented a technology solution to senior leadership and believed he had done a strong job. Afterward, one of the executives told him the presentation had not answered the questions leadership actually cared about.

What was the business value? What would it cost? What would happen if the organization did not make the investment?

"That was a big awakening moment for me when I realized that it's important to really talk from a business sense," Raj recalls.

Today, that experience shapes how he communicates with senior leaders and the board. Security risk has to be connected to business impact.

Kyle adds another element to executive communication: transparency. When he joined Avid, he did not try to make the security program appear stronger than it was.

"If I'm hiding that risk to make myself look better, that's a really bad place to be in," he says.

The common thread is that executive influence does not come from technical complexity. It comes from helping leadership

understand what matters, what it costs, and what the business may be exposed to.

AI IS PULLING SECURITY INTO THE BUSINESS EARLIER

If there is one force accelerating all of these changes, it is artificial intelligence.

The speed of AI adoption has disrupted the traditional security model. In many organizations, employees and business teams are gaining access to capabilities faster than governance teams can evaluate them.

Eric Bird describes 2026 as the era of "opt out, not opt in." His response has been to build stronger relationships with the people using the technology and lead with listening.

"What are you doing? How are you trying to do it? What can I learn from what you're doing as the user?"

That allows security and IT to understand the use case before determining what controls are necessary.

Sean is seeing the same phenomenon at CloudZero. AI is allowing people across the business to become builders, creating applications and automations that previously would have required a traditional development team.

"If you don't adapt with AI, you're going to lose," he explains.

The purpose of stronger governance is not simply to restrict the technology. It is to enable it safely.

Raj is dealing with AI adoption from multiple directions, including vendors embedding AI into existing products and business teams requesting new large language model tools. Northern Bank has established a governance committee to evaluate those requests and define standards for adoption.

The common thread is that AI governance is becoming less about writing a policy and more about creating an operating model. Security leaders need to understand what the business wants to accomplish, what data the use case requires, and what level of risk is acceptable.

That represents an important change in when security creates value. In the traditional model, a new technology might move through evaluation, procurement, and implementation before security became deeply involved. AI makes that increasingly difficult. The questions around data, access, third party technology, and acceptable use often need to be answered while the business is still deciding what it wants to build.

Getting involved earlier does not necessarily mean adding more checkpoints. In many cases, it means establishing relationships and expectations that allow decisions to move faster. Eric's emphasis on listening to users is one example. Raj's governance committee is another. Both approaches create a way for security to understand what is happening before it becomes a problem that needs to be unwound later. The strategic advantage is not simply better control. It is the ability to give the business a safer path forward without taking momentum away from innovation.

THE ANSWER IS INCREASINGLY NOT ANOTHER TOOL

Perhaps the most interesting theme across these interviews is how often leaders returned to the basics.

Cybersecurity is surrounded by new products promising to address AI risk, automation, identity, and data protection. Yet several leaders are actively resisting the assumption that the next improvement requires the next purchase.

Kyle has made this one of his primary priorities at Avid.

"We're not one tool away from making Avid more secure," he explains.

His focus is on maximizing the technology the organization already owns and addressing more systemic issues such as configuration management and process maturity.

"There are a lot of things that don't require a tool. It's just human work that has to be done."

Raj follows a similarly structured approach to vendor management, establishing requirements early and expecting vendors to meet those standards before moving forward.

That mindset also reflects a greater focus on getting more value from existing investments. Security leaders are under pressure to address a growing set of risks, but additional budget does not automatically translate into a stronger program. Technology still has to be configured correctly, integrated into existing processes, managed by people with the right expertise, and tied to a problem the organization actually needs to solve.

This becomes even more important as AI expands the number of products competing for security budgets. New capabilities can be valuable, but the interviews suggest leaders are becoming more deliberate about separating an emerging risk from an immediate purchasing decision. The first question is increasingly not, "What tool solves this?" It is, "What problem are we actually trying to solve?" That distinction can lead to a new investment, but it can also reveal an opportunity to improve a process, strengthen an existing control, or use technology the organization already owns more effectively.

The story is not that organizations should stop investing in technology. It is that technology is becoming one part of a more disciplined process: understand the business problem, determine the risk, evaluate existing capabilities, and then decide whether another investment is necessary.

SECURITY IS BECOMING A BUSINESS CAPABILITY

Taken together, these conversations point toward a broader transformation. Cybersecurity is becoming less of a function that sits beside the business and more of a capability embedded within how the organization operates.

Security leaders need to understand where the business is going before they determine what the program should prioritize. They need to communicate risk in a way executives can use to make decisions and help organizations adopt new technologies without becoming the barrier that slows them down.

At the same time, limited resources remain a reality. Raj described the challenge of addressing increasingly large risks with a lean security team. Salaam Harris, CISO at The Risk Management Foundation at the Harvard Medical Institutions, believes the people challenge is becoming even more important as AI expands.

“It would 100% go towards people,” Salaam says when asked where he would invest unlimited resources. “You can go buy more technology, but who’s going to manage that technology?”

AI can increase efficiency and help teams move faster, but it does not eliminate the need for judgment or strong leadership. If anything, the pace of change is making those qualities more important.

The strongest programs are increasingly the ones that begin with the business. They ask what the organization is trying to achieve, build security around those objectives, and translate risk in a way leaders can act on.

That may be the clearest picture of where cybersecurity leadership is headed. The security program of the future will still need strong technology and mature controls, but success will increasingly depend on how well those capabilities support the business and help leaders make better decisions.

K logix

1319 Beacon Street
Suite 1
Brookline, MA 02446

617.860.6485
KLOGIXSECURITY.COM

FEATS OF STRENGTH