A BUSINESS-FOCUSED CYBERSECURITY MAGAZINE JUNE 2026

FEATS OF STRENGTH

AI Governance

Guiding a course for responsible AI adoption.

FEATURING

Alastair Paterson
CEO and Co-Founder, Harmonic Security

Evan Wheeler
Senior Director Technology Risk Management, Capital One

Jay Mody
CISO, Chimera Investment Corporation

Rob Sherman
CISO, Lantheus

Sean Walls
SVP and CISO, Bob's Discount Furniture

Tope Iluyomade
Tech Expert and AI Advisor
Former CISO/CIO, BetterUp

IK logix

TABLE OF CONTENTS

FEATURES

JUNE 2026

LETTER FROM THE EDITOR

MAGAZINE CONTRIBUTORS

Katie Haug - Editor in Chief
VP Marketing, K logix

Kevin West - Editor
CEO, K logix

Emily Graumann - Graphics
Graphic Designer, K logix

ABOUT K LOGIX

Our white-glove approach empowers leaders to advance their security programs and strategically align with the business to reduce risk.

We craft our services to address specific customer and industry challenges. One of the ways we do this is through our thought leadership, business-focused publication *Feats of Strength*. Through hundreds of CISO interviews, we extract trends in order to provide services that align business to information security.

DEAR READERS,

As artificial intelligence continues to reshape the business landscape, the conversation is quickly moving beyond experimentation and into execution. Organizations are no longer asking whether AI will impact their business. They are focused on how to adopt it responsibly, govern it effectively, and ensure it delivers meaningful value. Across every interview in this issue, one theme emerged consistently: successful AI adoption is not about the technology alone. It is built on strong foundations of leadership, governance, data protection, and trust.

In this issue of Feats of Strength, we feature security leaders from a wide range of industries who are navigating these challenges in real time. Their perspectives highlight what it takes to lead through rapid change while balancing innovation with accountability. From AI governance and data security to resilience and operational readiness, these leaders are helping define the next chapter of cybersecurity. We hope their insights provide practical ideas, fresh perspectives, and inspiration as you build the future of security within your own organization.

Katie Haug

Editor in Chief

ALASTAIR PATERSON

CEO and Co-Founder

Harmonic Security

Headquarters: San Francisco, CA

Employees: 70+

Annual Revenue: Private Company, Series A Funding

PROFILES IN *Confidence*

For Alastair (Al) Paterson, building security companies has never been about reaching the destination. It is about the challenge of creating something that helps organizations solve real problems during periods of major change.

As a serial entrepreneur and cybersecurity leader, Al previously founded Digital Shadows, a threat intelligence company that grew to more than 500 enterprise customers before being acquired in 2022. After the acquisition, he found himself in an unfamiliar position.

"I'd gone from managing 160 people to zero," he recalls. "I thought the acquisition and destination was where I wanted to get. But I realized that I'd enjoyed building it, and that was where the real fun was. It's the journey as much as anything else."

That realization coincided with another major event. Just months after the acquisition, ChatGPT was released and organizations around the world began racing to understand what AI would mean for their businesses. For Al, the opportunity was immediately obvious.

"I became very passionate about the AI era very quickly," he explains. "My immediate reaction, given all my security heritage, was no enterprise is just going to roll this stuff out. They're going to need to get it live for competitive reasons, but there's going to be a whole host of security, legal, and compliance challenges around this."

That observation became the foundation for Harmonic Security. Founded in 2023, Harmonic helps organizations accelerate AI adoption safely by providing visibility, governance, and security controls across the rapidly expanding AI ecosystem. As enterprises embrace AI tools, agents, copilots, and automated workflows, Harmonic enables organizations to understand how AI is being used, where data is flowing, and how to apply the appropriate safeguards without slowing innovation.

For Al, the mission has remained consistent from day one. "I kept asking myself how we can help accelerate safe, fast AI adoption in the enterprise," he recalls. "That became the founding goal with Harmonic."

BUILDING FOR A MOVING TARGET

Unlike many cybersecurity categories that emerge around a specific problem, Al believes AI represents something fundamentally different. "This is not one of those times," Al observes. "The whole world is being hit with this AI tsunami, and security teams are having to become AI experts overnight."

That reality has shaped how Harmonic operates. When the company launched, the primary concern for many organizations centered on browser-based use of tools like ChatGPT and the risk of sensitive information being exposed through employee interactions. Since then, the landscape has evolved dramatically. AI capabilities have become embedded into enterprise applications and increasingly autonomous agentic systems.

As a result, Harmonic has had to evolve alongside the market. What began as a platform focused on AI-related data protection has expanded to address broader governance challenges, including agent management, prompt injection attacks, visibility into AI usage, and oversight of increasingly complex AI workflows.

"It isn't a static thing," Al notes. "We're seeing it move from browser usage to applications, to engineering workflows, to agents, and now cloud-hosted agents and team-based AI environments."

For many organizations, keeping pace with those changes has become one of the biggest challenges of AI adoption.

WHY TRADITIONAL SECURITY APPROACHES FALL SHORT

Al believes one of the biggest misconceptions organizations have is assuming AI can be managed using the same security approaches that worked in previous technology eras.

The challenge is not simply protecting data. It is understanding how employees interact with AI systems, how agents operate autonomously, and how sensitive information moves through increasingly dynamic environments. "Those are not things that

you can cover with the old world of rules and DLP from the previous era," he explains.

That belief has become one of Harmonic's primary differentiators. While many legacy vendors have added AI messaging to their existing platforms, AI believes the underlying technology was not built for how AI is actually being used today.

People no longer interact with technology through rigid workflows. They treat AI systems as advisors and collaborators, and as autonomous agents capable of performing actions on their behalf. AI comments, "You can't govern that with the prior generation's tools."

To address those challenges, Harmonic developed proprietary language models designed specifically to identify sensitive information, detect prompt injection attacks, and monitor potentially risky AI behavior. These capabilities allow organizations to move beyond traditional compliance-driven controls and gain visibility into how AI is being used across the enterprise.

"We're in a very different era now," AI notes. "People are feeding AI data in different forms, spinning up agents, and using these tools in ways we've never seen before."

TURNING SECURITY TEAMS INTO AI ENABLERS

As Harmonic has worked with organizations across financial services, healthcare, technology, and many other industries, one trend has become increasingly clear to AI. The most successful security leaders are not the ones trying to slow AI adoption. They are the ones helping the business embrace it responsibly.

"There's a tension between the business and the security organization," he explains. "The CEO may conclude that AI adoption is existential to the company and that they've got to move quickly."

In that environment, security teams face a choice. They can position themselves as obstacles, or they can become strategic partners helping the business move forward safely. AI sees a significant opportunity for security leaders who choose the latter.

"The huge career opportunity is for security teams to be AI native and pro AI enablement, and saying yes and leaning in," he emphasizes.

Increasingly, organizations are creating AI steering committees to guide adoption efforts. In many cases, CISOs are taking leadership roles within those groups, helping shape governance, risk management, and business strategy. For AI, that shift represents a broader evolution in the security profession.

"If you become known for being an enabler in AI and being very AI savvy, understanding what the tools do and using them yourselves while putting the right controls around it, that is one hell of a career opportunity," he points out.

He believes the future belongs to security leaders who spend time understanding how employees actually work and helping teams use AI more effectively. "If you say no, then the business is just going to stop asking you," he cautions.

LEADING AT THE SPEED OF AI

The pace of change in AI has also reshaped how AI thinks about leadership and company building. Unlike traditional software companies that can plan product roadmaps years in advance, Harmonic operates in an environment where major developments can emerge within weeks.

"The idea that you're going to build a twelve-month enterprise roadmap that you stick to is ridiculous for a company like us," AI explains. Instead, the company focuses on maintaining a clear mission while remaining agile enough to adapt as the market evolves.

Every week, the team evaluates what has changed in the AI landscape, what it means for customers, and how those developments should influence product direction. "We're very clear about what is changing in real time," he notes. "What does that mean for product? What does it mean for marketing? And what does it mean for our customers?"

That approach extends to the company culture as well. One of Harmonic's core values is what AI describes as flourishing in the unknown. Team members are encouraged to embrace uncertainty in order to adapt quickly, and to view ambiguity as an opportunity rather than an obstacle.

AI shared, "It's all about people that actually embrace the uncertainty and can function very quickly." For AI, that mindset is essential in an industry where change is constant.

THE NEXT CHAPTER OF AI ADOPTION

As organizations move beyond early experimentation, AI believes the conversation around AI is becoming more sophisticated. Initially, many discussions focused almost exclusively on risk. Today, leaders are asking different questions.

How is AI being used? Which teams are driving adoption? Where is the organization generating value? And what measurable business outcomes are being achieved?

To help answer those questions, Harmonic recently introduced capabilities designed to provide visibility into AI usage patterns across organizations. The goal is not simply to understand risk, but to help leaders understand adoption, enablement, and return on investment.

"This is becoming more than a risk conversation," AI points out. "It's becoming an enablement and ROI conversation as well." That evolution reflects what he sees across the broader market.

Organizations are no longer asking whether AI will become part of their business. They are trying to determine how to adopt it effectively, securely, and at scale. For AI, helping customers navigate that challenge remains the mission.

As the AI landscape continues to evolve, Harmonic's role is not to slow adoption, it is to help organizations move faster with confidence, providing the visibility and controls needed to embrace the opportunities of the AI era while managing the risks that come with it.

PROFILES IN *Confidence*

EVAN WHEELER

Senior Director Technology Risk Management

Capital One

Headquarters: McLean, Virginia

Employees: 76,300

Annual Revenue: $15.6 Billion

Evan Wheeler approaches cybersecurity through a risk lens, one that prioritizes business alignment and long-term decision making. At Capital One, he operates within the second line of defense, partnering closely with cybersecurity and technology teams while advising the business on how to manage and prioritize risk across a complex and evolving landscape.

His perspective reflects a broader evolution in the industry. Security is no longer just about controls and technology, it is about navigating ambiguity and making informed decisions in an environment where the pace of change continues to accelerate.

FROM CYBERSECURITY TO RISK LEADERSHIP

Evan's path into risk began with a gap. Early in his career, organizations were being asked to assess security risk, but there was no clear model for how to do it. "At the start of my career people started asking for security risk assessments, and there was no such thing," he explains.

Rather than relying on traditional approaches like vulnerability scans or penetration testing, he began building frameworks from scratch. "We started making it up on our own, looking at what risk assessments look like in other fields and trying to adapt it," he says.

That experience shaped his mindset that risk requires a different way of thinking. "It is a lot less absolute and a lot more about dealing with uncertainty and gray space," Evan explains.

For leaders who embrace that ambiguity, it creates a closer connection to the business and how decisions are actually made.

EXPANDING RISK BEYOND THE ENTERPRISE

Evan sees one of the biggest shifts in cybersecurity not within the organization itself, but in the expanding ecosystem around it. Risk is no longer contained within enterprise boundaries. It now extends across third and fourth parties, global operations, and interconnected systems that are increasingly difficult to track in real time.

What has changed most is not just the complexity, but the expectation of visibility. Boards and executives are no longer satisfied with understanding internal risk alone. They expect clear, immediate answers about exposure across regions and supply chains.

This shift has elevated the role of security and risk leaders. It is no longer enough to secure your own environment. Leaders must understand and account for dependencies they do not fully control, while still being able to explain that risk in a clear and actionable way.

For Evan, this is where the challenge lies. The ecosystem has grown faster than traditional approaches to managing it, forcing organizations to rethink how they measure, monitor, and communicate risk at scale.

THERE IS NO SINGLE CISO PLAYBOOK

One of the consistent themes Evan highlights is the diversity of leadership styles across the industry. "I do not find that there is any boilerplate CISO," he says.

Each leader brings a different perspective, shaped by their background and the needs of their organization. Some focus on product security, others on operations or strategy. The same is true for boards and executive teams. "They all have very different makeups and interests and priorities," he explains.

For Evan, this reinforces the importance of adaptability. Effective leaders surround themselves with diverse perspectives and tailor their approach to the environment they operate in.

INVESTING IN HIGH-LEVERAGE CONTROLS

In an environment of increasing complexity, Evan sees a clear shift toward prioritizing investments that deliver broad impact.

“We are all looking for where we can get the most leverage,” he says.

Rather than deploying point solutions, organizations are focusing on controls that reduce risk across multiple scenarios. Technologies like passwordless authentication and data tokenization stand out because they eliminate entire categories of threats rather than addressing a single issue.

“It does not just solve one threat vector, it solves across a whole gamut of things,” Evan explains.

This approach reflects a more strategic use of resources, where the goal is not to solve every problem individually, but to reduce risk at scale.

AI WILL ACCELERATE EVERYTHING

For Evan, the impact of AI is undeniable, even if the full implications are still unclear.

“I feel like I cannot quite imagine what two or five years ahead looks like,” he says.

What is clear is the speed. The time between discovering a vulnerability and seeing it exploited is shrinking rapidly. “It used to be weeks, now we are talking maybe hours or a day,” he explains.

At the same time, defenders are gaining new capabilities. AI can improve detection, response, and remediation, allowing organizations to move faster and operate more efficiently.

“I think both defenders and adversaries will mature at the same level,” Evan says.

For him, the dynamic is not about one side gaining an advantage, but about an acceleration on both sides. The result is a faster, more demanding environment where organizations must be ready to respond in real time.

AI AS A BUSINESS IMPERATIVE

One of the most notable shifts Evan highlights is how AI is being viewed within organizations. “The question from organizations always is, how can we get it faster?” he says.

Unlike previous technology waves, AI is not just an optimization, it is a business priority. “AI is really a business imperative,” he explains.

This changes the role of security. Instead of evaluating whether to adopt a technology, leaders must focus on how to enable it safely.

That requires clear guardrails and close collaboration with the business. It also requires trust that organizations can move quickly without compromising security.

BALANCING AUTOMATION AND TALENT DEVELOPMENT

As AI introduces new efficiencies, Evan is also thinking about its long-term impact on the workforce. “There is always going to be a need for experts,” he says, but he also raises a critical question about the pipeline of future talent.

If entry-level roles are reduced, organizations may struggle to develop the next generation of leaders. Over time, that could create gaps that are difficult to fill.

At the same time, AI creates opportunities to elevate existing roles. Tasks that were once manual can now be automated, allowing teams to focus on more strategic work.

“Right now, the only limits of AI is our imagination,” Evan says.

That balance between efficiency and development will be one of the defining challenges for security leaders in the years ahead.

THE FUNDAMENTALS STILL MATTER

Despite the rapid pace of change, Evan emphasizes that many core challenges remain the same. “The basics are really hard,” he says.

Issues like configuration management, process consistency, and root cause analysis continue to require significant effort and discipline. These are not simple problems, even if they are often described that way.

At the same time, he sees an opportunity to improve. Many of these processes are still manual and can be automated with the right approach. AI may finally make that possible at scale.

LOOKING AHEAD

When asked what will matter most in the near future, Evan is careful not to overstate certainty. “I do not know that I can picture a big shift,” he says.

What he does expect is continued acceleration. Organizations that embrace AI, apply it thoughtfully, and build the right guardrails will be better positioned to adapt.

He also sees the potential for AI to reshape how security tools work together, acting as a layer that connects and orchestrates across systems.

In many ways, the future remains undefined. But for Evan, one thing is clear. Success will depend less on predicting what comes next and more on building the ability to respond to it.

PROFILES IN *Confidence*

JAY MODY

CISO & Head of IT Infrastructure
Chimera Investment Corporation

Headquarters: New York, NY

Employees: 400+

Annual Revenue: Total revenues of $821 million and a GAAP net income of $144 million ($1.72 per diluted common share)

Jay Mody has spent nearly three decades evolving alongside technology itself. Over the course of a 28 year career spanning infrastructure, engineering, cybersecurity, and financial services, he has witnessed wave after wave of transformation. Through it all, one principle has remained consistent: security must enable the business, not slow it down. “I’ve always looked for gaps in business processes and controls, and tried to be proactive rather than reactive,” he says.

That mindset has shaped his leadership at Chimera Investment Corporation, where he serves in a dual role as both CISO and Head of IT Infrastructure. Since joining the company, Jay has helped guide Chimera through rapid growth, major acquisitions, evolving regulations, and the transition to a cloud-first environment, all while building a mature cybersecurity program designed to support the business as it scales. Jay sees his role as helping the organization grow securely while preparing for whatever comes next.

“I’m always trying to be a business enabler,” he says, “My goal is to let the business drive the car fast while making sure we have the right guardrails and brakes in place when needed.”

SECURITY AS A BUSINESS ENABLER

One of the defining shifts in Jay’s career came when he stopped viewing cybersecurity as purely a technical discipline and began aligning it directly with business priorities. “What are the challenges the business is facing? What is the CEO’s vision?” he says.

That perspective became especially important after Chimera brought in a new CEO focused on growth and acquisitions. Jay recalls a conversation where the company’s leadership made clear that expansion would move quickly and security needed to keep pace.

Rather than positioning cybersecurity as a blocker, Jay focused on demonstrating readiness. He highlighted the company’s investments in compliance, governance, and resilience while building new programs to support brand protection and digital trust.

One example involved protecting executive identities and the company’s public presence online. “I implemented a program to protect our digital brand,” he explains. “Making sure there is no impersonation and no lookalike domains out there.”

That business-first mindset now shapes how he approaches nearly every security initiative. Whether discussing infrastructure modernization, acquisitions, or AI adoption, the conversation always starts with business impact.

BUILDING AI AND DATA GOVERNANCE

As AI adoption accelerates across financial services, Jay is focused on ensuring governance evolves just as quickly. Two of his largest priorities today are AI governance and data governance, both of which he recently presented to senior management and the board.

“AI is something our CEO sees as essential,” Jay explains. “But he wants to make sure we have proper governance and guardrails.”

Jay approaches AI through three distinct lenses: AI as an asset, AI as a threat, and AI as a tool. That framework has helped structure how they evaluate risk and manage adoption across the organization.

At the center of the strategy is governance. Chimera established an AI task force that brings together stakeholders across enterprise risk, legal, business intelligence, and technology to define policies, training requirements, and

operational controls. “We need proper training. We need policy clearly defined,” he says. “Then the operations team can create the controls and processes based on those policies.”

The challenge, however, is the pace of change. Jay notes that vendors are increasingly embedding AI capabilities directly into enterprise platforms, often without customers actively requesting them. “They are already introducing AI features into their applications without asking anyone,” he comments.

For security leaders, that creates a difficult balance. Organizations cannot afford to fall behind, but they also cannot introduce AI without understanding the risks. “We don’t want to be left behind,” Jay shares. “But we also need to adapt our controls to this changing environment.”

To support that effort, they are using the NIST AI Risk Management Framework as the foundation for the governance strategy, while also implementing additional monitoring around AI agents and cloud environments.

PREPARING FOR AI-DRIVEN THREATS

While AI presents opportunities, Jay is equally focused on how it changes the threat landscape. One of the biggest concerns is how quickly attackers can weaponize vulnerabilities using advanced AI models. “Our response time is narrowing,” he reflects. “We used to get days to patch systems. Now as these models evolve, bad actors will eventually have access to these capabilities as well.”

His response centers on two priorities: response time and resiliency. Jay’s team focuses heavily on protecting internet-facing systems through continuous threat exposure management while maintaining strong internal segmentation and zero-trust controls. But he also recognizes that prevention alone is not enough.

“If a bad actor breaches our network and brings systems down, I’m going to rely on our established backup and disaster recovery process,” he explains. That preparation is something Chimera has invested in for years. Jay emphasizes that resiliency is not built during a crisis. It must already exist before one occurs.

“My team is prepared to respond to any breach or ransomware threat,” he stresses. He also sees AI playing a growing role in recovery itself. They are implementing AI-driven recovery capabilities designed to identify the safest restore points following an incident, reducing recovery time during a potential attack.

SCALING SECURITY THROUGH GROWTH AND ACQUISITION

The company’s recent acquisitions introduced another major challenge: integrating organizations with very different levels of security maturity. Rather than immediately imposing controls, Jay focused first on awareness and alignment. “These are the gaps we identified in your environment,” he recalls telling leadership teams. “Here’s the roadmap to bring you into Chimera’s secure operating environment.”

That roadmap included deploying visibility tools, integrating vulnerability management, and aligning systems with the controls already established within Chimera’s environment.

Jay approached both situations the same way: transparency, collaboration, and education. “Technology evolves. Risk evolves,” he explains. “It’s a changing landscape.”

LEADING THROUGH COLLABORATION AND ACCOUNTABILITY

Jay describes his leadership style as collaborative and execution focused. “I want my team to collaborate and work across the business,” he says. “The business needs to understand why we are doing this and where the end state will be.”

He also emphasizes accountability. For Jay, projects are not complete when technology is deployed. They are complete only after monitoring, backup, disaster recovery, compliance integration, and documentation are fully operational. “I don’t want someone telling me the project is done,” he says. “I want to know the monitoring is in place, the backup is configured, and the documentation is complete.”

At the same time, he is intentionally preparing his team for larger leadership opportunities by gradually giving them ownership over critical systems and initiatives. He comments, “Many team members want to grow and work on different technologies, so I’m giving them more responsibility as they develop.” That investment in people mirrors the support Jay says he has received throughout his own career.

Since joining the organization, he has grown from Director of Infrastructure to CISO and Head of IT Infrastructure, gaining direct access to executive leadership and the board along the way.

“They’ve given me that growth ladder,” he says. “I have a seat at the table, and I can share risk very transparently.” For Jay, that transparency is essential to effective leadership, especially as AI, cloud adoption, and cyber risk continue to evolve simultaneously.

The pace of change may continue to accelerate, but his focus remains consistent: build resilient systems, support the business, and prepare the organization for what comes next.

PROFILES IN *Confidence*

ROB SHERMAN

CISO

Lantheus

Headquarters: Bedford, MA

Employees: 1,000+

Annual Revenue: $1.54 Billion

After spending 24 years at American Tower helping build and scale a global security program, Rob Sherman was not looking for just another CISO role, he was looking for an opportunity to build something meaningful.

"When I talked to recruiters, I told them if you've got a role where the CISO had just left and they're looking for someone to backfill and they're pretty happy with their program, don't call me," he recalls. "I'm looking to build or re-build a security program and really get my hands dirty."

That search ultimately led him to Lantheus, the leading radiopharmaceutical-focused company committed to enabling clinicians to Find, Fight and Follow disease to deliver better patient outcomes. The opportunity checked every box. The company was growing rapidly, expanding internationally, and looking to establish its first dedicated security leadership role.

"They wanted someone to come in and build a program," Rob shares. "To me that really sounded like fun."

What began as an opportunity to build a security program soon became something more personal. Just weeks into the role, Rob experienced a weekend data center outage that changed his perspective on the business. While coordinating updates during the incident, he learned that if systems were not restored quickly, health care facilities could be forced to cancel patient appointments.

Rob's recognition of the organization's impact was immediate, he quickly realized that every system, process, and security control ultimately supported patients waiting for critical diagnostic scans. "The company's purpose really hit me," he reflects. "What we're doing is directly impacting patient care."

BUILDING A PROGRAM WITH PURPOSE

Having built programs before, Rob resisted the temptation to arrive with a predetermined playbook. He explains, "I didn't want to be that guy who comes in with all my smart ideas from my other company and steamroll everything."

Instead, he spent his first months listening. He met with stakeholders across the organization, studied existing processes, and worked to understand why decisions had been made.

As a public company, Lantheus already had many security controls and technologies in place. What was needed was an overarching strategy to tie them together. The early stages of the program focused on rationalizing tools, identifying gaps, simplifying overlapping technologies, and creating a roadmap aligned to business priorities. Rather than replacing everything, Rob focused on building a cohesive program that could support the company's continued growth.

COMMUNICATING WITH LEADERSHIP

Building the program required more than technology decisions, it also required earning trust with executives and the Board. Fortunately, Rob gained valuable insight into the organization's leadership style during the interview process, particularly through conversations with the CFO and General Counsel.

When presenting to the Board, Rob combines updates on Lantheus' security program with discussions about broader industry developments. He wants executives to understand not only what is happening inside the company, but also how emerging threats and trends could impact the business.

"I find Board members are typically on multiple Boards," he notes. "They hear a lot of things, and they read a lot of things,

so I need to be prepared to answer a broad range of questions." This approach has helped create productive conversations rooted in business context rather than technical details.

GROWTH AND AI

Today, one of the company's largest priorities is integrating acquisitions. Lantheus has completed multiple acquisitions since Rob joined, making integration a central focus for both the business and the security team. Alongside those efforts, the organization continues progressing toward a zero-trust architecture built around a select group of strategic platforms. For Rob, simplification matters.

He comments, "We've picked our platform vendors, and we're just making sure that we've got as many tools as possible in that platform turned on, tuned, and running optimally."

AI is another area receiving significant attention, though Rob believes the conversation is still evolving. Like many organizations, Lantheus uses AI tools to improve productivity. The bigger question, however, is how AI can create measurable value within security operations.

"I really want to figure out where we can effectively use AI to make a material difference in how we're running our cyber organization," he explains.

While many companies are racing to establish AI governance frameworks, Rob sees substantial overlap between AI governance and the security governance programs organizations have been building for years. "There are a lot of elements of AI governance that overlap very heavily in my mind with what we've done for years and years with cyber governance," he says.

For now, his approach is practical. Lantheus has updated policies, provided employee training, and strengthened oversight through existing third-party risk management processes while continuing to evaluate future AI use cases.

LEADING WITH IMPACT

Moving from a large global organization to a smaller, fast-growing company has changed the nature of Rob's role. On any given day, he may move from technical architecture discussions to executive presentations within the span of an hour.

"The CISO role in a small organization spans a much broader range," he comments. That breadth is one of the reasons he enjoys the environment.

Early in his career, Rob realized he was motivated by opportunities to solve problems and contribute across the business. Smaller organizations provide more opportunities to do exactly that. He notes, "I like environments where I have an impact and in a smaller environment you usually have more opportunities to make more of an impact."

As Lantheus continues to grow, Rob remains focused on building a security program that enables the business while supporting a purpose that extends far beyond technology. For him, security is not just about protecting systems, it is about ensuring that patients, physicians, and healthcare providers can depend on the critical services that Lantheus delivers every day.

PROFILES IN *Confidence*

SEAN WALLS

SVP & CISO

Bob's Discount Furniture

Headquarters: Manchester, CT

Employees: 5,950

Annual Revenue: $2.4 Billion

For Sean Walls, career growth has rarely come from staying comfortable. Over the past several years, his journey has taken him from Pennsylvania to Texas and now Connecticut, across multiple leadership roles, through mergers and acquisitions, and ultimately to Bob's Discount Furniture, where he now serves as Senior Vice President, Chief Information Security Officer. Along the way, he has built security programs and helped organizations adapt during periods of significant change.

"If you're really serious about growing and developing, you're going to take opportunities that sometimes are risky and force you to move," Sean says. "I think if it's the right opportunity, then taking that risk makes sense."

That philosophy has shaped much of his career. Following his time at Visionworks (the last time Sean was featured in the Feats of Strength magazine), Sean moved into a larger leadership role, overseeing security across several business units while leading governance, risk, and compliance initiatives for the broader organization. Later, he joined Conn's HomePlus, where he helped oversee security through a major acquisition before the company ultimately faced financial challenges and filed Chapter 11.

Then, a former colleague connected him with the leadership team at Bob's Discount Furniture. Within days, Sean was interviewing with executives and by the end of the week, he had an offer in hand. Today, he leads security for this fast growing furniture retailer, helping guide the company through rapid expansion and an increasingly complex technology landscape.

SECURITY AS A BUSINESS FUNCTION

Sean joined Bob's shortly before the company's public offering, making it a pivotal moment for both the business and the security program.

As the company's first dedicated CISO, he was brought in to elevate security as a standalone executive function and help prepare the organization for its next stage of growth.

"This is the first official CISO role," Sean explains. His responsibilities extend well beyond traditional cybersecurity. In addition to information security, he oversees governance, risk management, compliance, privacy, business continuity, crisis management, and related operational functions.

For Sean, that broader scope creates a significant advantage. When security leaders understand compliance, resiliency, and risk as part of a larger business ecosystem, they are better positioned to influence decisions and drive meaningful change. He comments, "You can see the bigger picture, you understand the strategy, and you can affect change within your circles of influence."

That ability to connect security priorities to business objectives has become one of the defining themes of his leadership philosophy.

SPEAKING THE LANGUAGE OF THE BUSINESS

While many security leaders aspire to gain executive visibility, Sean believes influence is earned through communication, relationships, and trust.

"The first thing that you need to do when you arrive on your first day is develop relationships with key stakeholders within the organization," he says. For him, technical expertise alone is not enough. The most successful CISOs understand how to communicate risk in terms that resonate with business leaders.

"If it doesn't include conversations around dollars, profit, savings, and return on investment, then you're missing the mark completely," Sean explains. That perspective reflects how much the role has evolved over the past decade.

Security leaders are no longer viewed as gatekeepers whose primary responsibility is saying no. Instead, they are expected to help organizations move faster and pursue innovation while managing risk appropriately.

"We're not here to say no," Sean says. "We're here to empower and strengthen the business." He believes mature security programs can become competitive advantages, helping organizations operate more efficiently while maintaining the governance structures necessary to support growth.

NAVIGATING AN ERA OF SIMULTANEOUS CHANGE

One of the biggest challenges Sean sees today is not a single threat or technology, but the fact that, as he puts it, "everything is changing at the same time." Organizations are navigating rapid business growth, expanding regulatory requirements, accelerating technology adoption, and an increasingly sophisticated threat landscape, often simultaneously.

For Bob's, that includes managing the responsibilities that come with being a public company that continues to expand rapidly across the United States. And at the same time, AI is reshaping both sides of the security equation.

Sean sees enormous opportunities for organizations to leverage AI to improve efficiency and create competitive advantages. But he also recognizes that attackers now have access to increasingly powerful tools.

One development that has captured significant attention is the emergence of advanced AI systems capable of identifying vulnerabilities, creating exploits, and accelerating attacks. "The kill chain is about to be compressed significantly," Sean says.

As a result, many long-standing assumptions about cybersecurity operations are being challenged. Organizations can no longer rely on traditional response timelines. Detection, investigation, and remediation must happen much faster than they did in the past.

"We're not talking in one-month patch cycles anymore," he explains. "We're talking real-time patching." That shift is forcing security leaders to rethink everything from vulnerability management to incident response.

AI GOVERNANCE AND THE FUTURE OF SECURITY

Like many of his peers, Sean spends a significant amount of time discussing AI governance. From his perspective, security leaders recognize that they are living through a transformational period that will reshape industries and organizations alike.

"The entire world is going to transform in the next five years in ways that will leave it almost unrecognizable," he explains. And the conversations he has with fellow CISOs reflect that reality.

As a member of several advisory boards, Sean regularly engages with security leaders across industries. While organizations may vary in maturity, he sees widespread awareness of the challenges and opportunities ahead. "This is all people are talking about right now," he notes.

For security teams, the challenge is finding the right balance between enabling innovation and maintaining control. Organizations want to take advantage of AI's potential, but they must do so in a way that protects data and manages emerging risks. That balance will likely define the next chapter of cybersecurity leadership.

BUILDING TEAMS THAT GROW

While technology continues to evolve, Sean believes leadership remains fundamentally about people.

He describes himself as a transformational leader who enjoys building programs and helping organizations mature. But he is equally passionate about developing the people around him. "I've always considered myself a builder and a fixer," he comments.

Sean intentionally gives team members opportunities to get out of their comfort zones. Growth, in his view, comes from experience, challenges, and learning through real-world situations. "I like to encourage people to stretch themselves," he says.

At the same time, he recognizes that every employee requires a different leadership approach. Some need autonomy while others need coaching and support as they develop new skills. His role is to understand those differences and invest accordingly. "As long as somebody's willing to learn and to grow, I am willing to invest in them," Sean says.

That philosophy mirrors his own career journey. From consulting and security leadership to mergers, acquisitions, and public company governance, Sean has consistently embraced opportunities to grow and adapt.

Today, as Bob's Discount Furniture continues to expand, he remains focused on helping the organization navigate a rapidly changing landscape while ensuring security remains a catalyst for growth rather than a barrier to it.

PROFILES IN *Confidence*

TOPE ILUYOMADE

Technology Executive and AI Advisor

Former:
CIO/CISO, BetterUp
VP of Business Technology, Marqeta
CISO, Aera Technology

Technology has shaped nearly every part of Tope Iluyomade's life and career. Long before he became a CIO/CISO and advisor helping organizations navigate AI and cybersecurity, he was a child learning English on a Macintosh computer. "Technology has really helped me personally grow up as a person," he says. "I learned to speak English on a Macintosh."

That early fascination with innovation led him into robotics, software engineering, and eventually AI, nearly two decades ago while studying at the University of Maryland Baltimore County. Working on early AI systems in financial services quickly introduced him to the realities of cybersecurity. "When you're doing early AI and working on Wall Street, naturally cybersecurity came up," he explains. "How do we secure these systems, especially when hundreds of billions and trillions of dollars would be going through it?"

Throughout his career, Tope has worked across aviation, fintech, supply chain, healthcare, and mental health technology, building a unique perspective that combines technical depth with business leadership. He credits much of his growth to mentors who helped shape how he thinks about leadership and resilience.

One of the defining experiences early in his career came while supporting cyber incident response efforts for organizations connected to the Department of Defense. He says, "We had 24 hours to contain a security breach, redesign the architecture for the company, work with legal, learn policies, and so much more. It was an amazing crash course on cybersecurity when it really mattered."

That intensity helped build the foundation for how he approaches leadership today: staying calm under pressure by understanding the business impact and focusing on the decisions that matter most.

LEARNING TO SPEAK THE LANGUAGE OF THE BUSINESS

As Tope progressed into leadership roles, he learned that technical expertise alone was not enough, an important lesson that would stick with him in his career.

After moving from the East Coast to the West Coast and joining Alaska Airlines, he gained his first experience working closely with boards and executive leadership. The shift forced him to rethink how he communicated security.

"To succeed at the executive level, security leaders have to translate technical concepts into business priorities that people understand and engage with," he says.

That transition did not happen automatically. Tope describes it as a deliberate process of self-awareness and learning from other leaders across the business.

"I noticed that I tended to focus on the technical at first, and there were things I didn't realize were jargon to nontechnical people, so I had to adjust my self-awareness of how I was sharing information," he explains.

Rather than staying within the security function, he spent time learning how different teams operated and what mattered to them. "To be successful at this level, you need to be able to put yourself in different perspectives from across the business," he says. "Sales is trying to make sure revenue's coming in. The CFO's trying to make sure profitability is within range or else the business doesn't exist."

That mindset fundamentally changed how he approached leadership. Instead of treating security as a separate function, he began framing it in terms of business outcomes and customer trust.

He also credits CFOs with helping him develop that perspective. "The CFOs are the language translators for every function to the board," he says. "I've learned to speak in terms of profitability, and that has really helped me."

For security leaders looking to move into executive roles, Tope believes relationship building is essential.

"It's better to get fifty percent of what you want than zero," he says. "Most security leaders try to translate up to the CFO. That's

backward. Find the analyst on the finance team who builds the board deck and learn their model. By the time you reach the CFO, you're not translating anymore. You're already in the conversation."

LEADERSHIP DURING CRISIS

Some of the most formative moments in Tope's career came during the COVID-19 pandemic while serving at Aera Technology, where the company supported AI-driven supply chain operations for organizations including Unilever, Merck, Pfizer, and Johnson & Johnson.

Before the pandemic, supply chain optimization was important, but during COVID, it became mission critical.

"In March 2020, we rewrote the fulfillment logic from 'highest-value order first' to round-robin distribution. The math was trivial. The decision wasn't. That single change determined which communities got vaccines in the first wave. It's the moment I realized security and supply chain leadership are the same job in a crisis: deciding who gets protected first, with imperfect information, under time pressure."

That insight, that crisis leadership is fundamentally a question of triage under uncertainty, became a throughline in how he approached every role that followed.

AI MOVES FROM EXPERIMENTATION TO ACCOUNTABILITY

Today, as Tope looks across industries, he sees organizations entering a new phase of AI adoption. He comments that last year the priority was experimentation, and this year the focus has shifted to measurable business value.

"The challenge last year was the bias toward experimentation," he explains. "The board didn't want to be left behind. They encouraged teams to experiment with as many AI tools as possible."

Now, organizations are facing more pressure to justify those investments. "This year, what I'm seeing is the chicken has come home to roost," he says. "You've spent that money, now tell me what it's done to my P&L impact."

Tope believes many organizations are struggling to connect AI initiatives to measurable economic outcomes. The excitement around AI remains high, but leaders are now expected to demonstrate tangible results.

His advice is to focus on targeted, high-impact use cases instead of broad experimentation. "Choose a use case that is a very clear about the value, then do it over again and expand," he says. "This works better than starting with a wide harvesting approach."

He also sees workforce readiness as one of the biggest gaps facing organizations today. While companies are moving quickly to adopt AI, many are not investing at the same pace in training their employees to use it effectively and responsibly. Tope points out that most organizations still lack the structure and long-term commitment needed to properly develop those skills at scale. For him, successful AI adoption is not just about deploying tools. It requires enabling employees to understand how to use them responsibly and effectively.

RETHINKING AI GOVERNANCE

Tope believes the governance conversation is rapidly evolving. He says that last year, many organizations focused on establishing AI councils and oversight groups. Today, the challenge is operationalizing those efforts in a way that does not slow down the business.

"Fortune 100 companies stood up AI councils to review strategy," he says. "But this year, what you're going to see is that CEOs and councils should not be involved in every AI decision."

Instead, governance must become embedded into day-to-day operations and workflows. "If you have to go through a council or read a document to instrument safeguards, it's not going to work," Tope explains. "You need to build in-the-flow-of-work governance for these AI tools to make sense."

He compares the current state of AI governance to the development of brakes in automobiles. Governance should not exist to slow organizations down. It should exist to make innovation safer and more scalable.

"If you and I didn't have brakes in cars, we would never go over the speed limit," he says. "We are able to speed because we trust the safety of the brakes."

That philosophy extends beyond internal governance and into third-party risk management, procurement, and regulatory oversight. Organizations are increasingly asking where AI is being used and whether vendors are operating within public or private environments.

"What can I use to make sure this tool doesn't deviate from what we signed up for?" he says. "Last year reactive was fine. This year proactive is necessary."

BUILDING WHAT COMES NEXT

Tope is entering a new chapter focused on board advisory work and building a company of his own.

He says, "After a career inside security and technology organizations, I've watched most AI investment go to the enterprises that least need help affording it. The gap I'm focused on is the middle market: companies with real operational complexity but without the budget or staff for enterprise AI tooling. That's where I think the next decade of meaningful AI adoption happens, and where two decades of operating at the intersection of security, infrastructure, and enterprise systems translate most directly."

That shift is what excites him most. Not just the technology itself, but the opportunity to rethink how systems, people, and organizations interact.

As AI continues to evolve, Tope believes leadership will become even more important. For him, the future belongs to leaders who can balance innovation with accountability and move beyond fear-driven conversations about AI. "The world is going to be rewired around it," he says. "So I'm making a big pivot in my career to be at the forefront of that and apply it to the right places that matter."

The AI Governance Imperative

Building Structure in an Era of Accelerated Adoption

Artificial intelligence has moved far beyond experimentation. What began as isolated testing of generative AI tools has quickly evolved into enterprise wide adoption. As we have been part of the AI journey with many of our customers, we have observed that organizations are using AI to improve productivity, automate workflows, enhance security operations, and accelerate business initiatives. As adoption continues to expand, many organizations are discovering that innovation is moving faster than oversight.

According to K logix observations, over two thirds of security leaders report having some form of AI governance committee or oversight group in place. While this represents an important first step, many organizations are still determining how to transform discussions into repeatable processes and policies.

To better understand how organizations are approaching AI governance, we spoke with Sydney Gelb, Senior Manager at K logix and Sydney Solomon, West Coast Practice Lead at K logix, who help organizations navigate a rapidly evolving AI regulatory and compliance landscape and translate it into actionable governance and security initiatives they can implement.

WHEN AI BECOMES IMPOSSIBLE TO IGNORE

Many organizations entered the AI era cautiously. Initial efforts are often centered on employee experimentation with tools such as ChatGPT, Claude, and Microsoft Copilot. What started as individual productivity gains soon expanded into business functions ranging from software development and customer service to security operations and compliance.

As AI capabilities became embedded in everyday workflows, governance became increasingly difficult to postpone. “Governance becomes a priority when an unknown like AI begins to take shape within organizational agendas and becomes impossible to ignore,” says Gelb.

Today, AI is no longer viewed as a standalone technology initiative. It is becoming a new operational and security domain that requires defined ownership and controls.

“AI governance is an amalgamation of strategy, legal and regulatory compliance, leadership oversight, and risk management related to the use of AI at an organization,” Gelb explains. “AI itself is a risk, so I like to think of AI governance as a dedicated risk management program specific to artificial intelligence.”

Organizations that fail to establish governance frameworks risk creating environments where AI adoption expands without visibility into how tools are being used, what data is being shared, and who is responsible for managing associated risks.

THE RISKS BEHIND RAPID ADOPTION

For many organizations, the greatest challenge is not that AI introduces entirely new risks. Rather, it amplifies existing concerns around data security, privacy, compliance, and governance. Among the most common concerns raised by security leaders is the potential for sensitive data exposure.

“The biggest risk we hear from customers pertains to data loss,” Gelb explains. “Organizations need to ensure their data is appropriately identified, classified, and tagged to prevent misuse or undetected sensitive data ingestion into unlicensed tools.”

As AI systems gain access to larger volumes of organizational data, traditional governance practices become increasingly important. Data classification, access management, vendor oversight, and user education all play critical roles in reducing exposure.

At the same time, organizations are facing pressure from executives and boards seeking assurance that AI initiatives are being implemented responsibly. The challenge is compounded by the speed at which adoption is occurring. In many cases, business units are deploying AI capabilities faster than governance teams can assess and monitor them.

WHAT ORGANIZATIONS ARE DOING TODAY

While AI governance programs remain relatively immature across many industries, clear trends are emerging.

The K logix team has observed that organizations are increasingly using AI copilots to assist with document analysis, content generation, and workflow automation. Security teams are leveraging AI powered detection and response capabilities delivered through managed service providers. Compliance and audit teams are beginning to explore AI as a means of centralizing evidence collection and streamlining assessments.

These use cases offer significant efficiency gains, but they also expand the attack surface and introduce new governance requirements.

As organizations scale AI initiatives, security leaders are recognizing that successful adoption requires more than technology controls. It requires a framework that aligns AI initiatives with business objectives, risk tolerance, and compliance obligations.

THE GOVERNANCE GAP

One of the most common misconceptions Gelb encounters is the belief that governance can be addressed through documentation alone. She comments, "Some organizations view AI governance as simply a change of paper. If we have a policy, we're protected. But that's not the case."

Policies are important, but they represent only one component of a successful governance program. Organizations must also establish awareness, training, accountability, and oversight mechanisms that influence behavior across the enterprise.

"It requires awareness and training across the organization to mitigate risks like insider threat and data loss," Gelb says. "Educating users on how to use AI and when human intervention is needed is critical to ensuring it is used securely."

Governance must also extend beyond security teams. Organizations need visibility into all AI systems, applications, and third-party services operating across the business. Without proper inventory and oversight, organizations may struggle to understand where AI is being used and what risks it introduces.

A NEW REGULATORY REALITY

As organizations mature their governance programs, they are increasingly looking to established frameworks and emerging regulations for guidance.

According to Solomon, "The NIST AI Risk Management Framework is one of the more useful starting points for organizations because it helps turn AI governance from an abstract concept into something operational. By organizing risk management around the four NIST functions, govern, map, measure, and manage, the framework provides teams with a common structure for understanding where AI risks arise across the AI lifecycle, assessing those risks, and building governance

processes that can evolve alongside the technology."

Global regulations are also evolving rapidly. The European Union's AI Act, which entered into force in 2024 and introduces obligations in phases through 2026 and beyond, establishes a risk based approach to regulating AI systems and is expected to influence governance programs worldwide.

At the same time, standards such as ISO/IEC 42001 are providing organizations with structured guidance for managing AI systems responsibly throughout their lifecycle, while helping prepare for evolving regulatory expectations.

Even within the United States, where there is no comprehensive federal AI law, states such as California are helping shape the future of AI governance. Solomon, who resides in California, states "California is a good example of how quickly AI governance is moving into real-world compliance expectations. Recent privacy and AI developments here point to growing regulatory focus on transparency, the protection of personal information in AI systems, and automated decision-making." For security leaders, these developments signal that AI governance is rapidly becoming a business requirement rather than a future consideration.

WHERE ORGANIZATIONS SHOULD START

Despite the complexity of the challenge, Gelb advises organizations not to overcomplicate the first steps. She notes, "AI governance starts at the top of the organization, with buy in from business and security leaders to understand how AI will be used and who is responsible for managing it."

From there, organizations should establish a governance committee responsible for defining guardrails, reviewing proposed AI initiatives, and creating processes for evaluating risk. "It can often be useful to bring in an external perspective early to ensure all considerations are addressed proactively rather than retroactively," she describes.

Ultimately, successful governance programs combine visibility, accountability, and education with a clear understanding of organizational goals. "The most difficult part of building an AI program is knowing where to start," says Gelb. "Having the right expertise helps organizations develop a roadmap and move forward with confidence."

FIVE STEPS TO BUILDING AN AI GOVERNANCE FOUNDATION

For organizations just beginning their AI governance journey, both Gelb and Solomon emphasize that progress does not require a fully mature program from day one. As Solomon states, "What matters most is creating a foundation strong enough to support responsible AI adoption today but flexible enough to adapt as AI use-cases evolve, business priorities shift, and regulatory expectations continue to take shape."

1. Establish Executive Ownership

AI governance cannot be delegated solely to security or IT teams. Organizations should identify executive sponsors and define clear accountability for AI related decision making.

"AI governance starts at the top of the organization," says Gelb. "Leadership alignment is critical because AI impacts far more than technology. It affects business processes, risk management, legal considerations, and compliance."

2. Create an AI Governance Committee

Many successful organizations begin by forming a cross functional governance group that includes representatives from security, legal, compliance, privacy, risk management, and business operations.

The committee should be responsible for defining acceptable use guidelines, reviewing new AI initiatives, and establishing oversight processes that align with organizational goals.

3. Gain Visibility Into AI Usage

Organizations cannot govern what they do not know exists.

This means identifying approved and unapproved AI tools, understanding where AI capabilities exist within third-party platforms, and maintaining an inventory of AI systems being used throughout the organization.

Without visibility, organizations may unknowingly expose sensitive information, create compliance challenges, or increase operational risk.

4. Develop Policies, Training, and Guardrails

While policies alone are not enough, they remain an important component of governance.

Organizations should establish clear guidance around:

- Approved AI use cases
- Data handling requirements
- Human review expectations
- Third-party AI usage
- Employee responsibilities

Equally important is ongoing education to help employees understand both the benefits and limitations of AI technologies.

5. Align to Recognized Frameworks

Organizations do not need to build governance programs from scratch.

Frameworks such as the NIST AI RMF and ISO/IEC 42001 provide practical guidance for establishing governance structures, assessing risk, and preparing for future regulatory requirements.

According to Solomon, “Organizations don’t need to build AI governance from scratch. Established frameworks provide a practical path forward, helping teams mature their governance program while keeping it aligned with emerging regulatory expectations and industry best practices.”

TURNING AI INTO A SUSTAINABLE BUSINESS CAPABILITY

As AI adoption continues to accelerate, organizations that establish governance early will be better positioned to innovate responsibly, satisfy evolving regulatory expectations, and build sustainable AI programs that support long term business objectives.

While many leaders are still determining where to begin, one thing is becoming increasingly clear: AI governance is no longer a future initiative. It is rapidly becoming a core component of cybersecurity, risk management, and business strategy.

“The conversation around AI is often focused on what’s possible,” says Solomon. “But for organizations, the more important question is whether they are prepared to manage it responsibly. Governance is what turns AI from an experiment into a sustainable business capability.”

CONCLUSION

While these foundational steps provide a starting point, AI governance is ultimately a journey rather than a destination. As adoption continues to accelerate, organizations that establish governance early will be better positioned to innovate responsibly, satisfy evolving regulatory expectations, and build sustainable AI programs that support long term business objectives.

K logix

1319 Beacon Street
Suite 1
Brookline, MA 02446

617.860.6485
KLOGIXSECURITY.COM