June 2025

FEATS OF STRENGTH

A BUSINESS-FOCUSED CYBERSECURITY MAGAZINE

CYBER TRENDS

The Year of AI Security, Identity Hardening, and Resilience Scaling

HEAR FROM CISOs & SECURITY LEADERS AT:

AUDITBOARD
CRUM & FORSTER
MARSH McLENNAN
NAVY FEDERAL CREDIT UNION
NESTLE PURINA
PURE STORAGE
SCHNEIDER ELECTRIC
SEVEN HILL VENTURES
SYN VENTURES
& More

K logix

TABLE OF CONTENTS

FEATURES

June 2025

MAGAZINE CONTRIBUTORS

Katie Haug - Editor
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.

CISO Perspectives 2025: Trends Reshaping Cybersecurity

By Katie Haug

In a year marked by rapid technological acceleration and heightened digital risk, CISOs find themselves at a critical junction. We had conversations with more than 20 cybersecurity leaders from diverse sectors, and their responses are included in this article. The thoughtful feedback from these leads revealed not only a shared set of concerns but also a roadmap to resilience in 2025 and beyond. From artificial intelligence to board engagement and identity governance, this article unpacks the top trends that will shape CISO priorities over the next year.

AI: OPPORTUNITY AND URGENCY

AI stands out as both an innovation enabler and a cyber risk multiplier. As CISOs adopt internal AI tools for compliance, IT automation, and employee productivity, they simultaneously grapple with new threats like deepfakes, prompt injection, and agentic AI misuse.

> "There's a good strain that's placed on me and that is to become more educated around AI."
>
> – Dan Bowden, Global CISO, Marsh McLennan

Shadow AI is rising as employees adopt tools like ChatGPT, Grammarly, and internal copilots before policies can catch up. This introduces visibility, privacy, and compliance challenges. Trust in digital communication is also eroding, as deepfakes and impersonation tactics grow more convincing.

To manage this complexity, many CISOs anticipate the emergence of AI-specific roles focused on governance and risk management. The pressure is also on security teams to quickly educate themselves on foundational AI concepts, major platform architectures, and evolving regulatory guidance. Many CISOs emphasized the need for continuous learning, experimentation, and internal R&D as core components of their AI readiness.

Additionally, CISOs are finding that enabling safe AI adoption creates a compelling opportunity to reposition security as a business enabler. By proactively working with product and operations teams to vet AI vendors, obtain enterprise licenses, and monitor usage, security leaders are able to shift from "gatekeeper" to "strategic partner."

IDENTITY SPRAWL

Machine identities, SaaS integrations, and ephemeral cloud services have led to an explosion in identity sprawl. This growth threatens visibility and increases the likelihood of privilege misuse. Simultaneously, organizations are prioritizing scalable and cost-efficient logging infrastructures.

Furthermore, legacy tech debt and cloud migration continue to challenge foundational security postures.

> "We were very heavy on prem, now we're moving to a lot more cloud... You have to develop a new shared responsibility model."
>
> – Michael Newborn, CISO, Navy Federal Credit Union

To address these challenges, CISOs are increasingly adopting a problem-first mindset. Instead of focusing on a specific product or vendor, many are working to define capability gaps first, then examining existing toolsets and identifying where open-source or cross-functional solutions might apply. Only after this internal analysis do they proceed to evaluate external vendors. This approach is helping teams rein in sprawl and avoid duplicate or underutilized tools.

Security teams are also paying more attention to vendor lifecycle management, reassessing past purchases to determine whether tools still deliver value or should be replaced. This continuous scrutiny ensures tighter alignment between security investments and evolving business needs.

SECURITY KEEPING PACE WITH BUSINESS

Security programs are often struggling to match the speed of digital transformation. A shift is underway as CISOs try to bring their strategies closer to core business goals.

> “With the objectives of security, I think we are trying to move in lockstep with what the business is doing all the time.”
>
> – Heather Reed, Head of Cybersecurity, Nestlé Purina PetCare North America

Vendor sprawl is being addressed through platform consolidation, with CISOs looking for fewer, more interoperable tools. Some organizations are now achieving true business/security alignment, reporting improved collaboration and clearer priorities.

Conversely, GRC and traditional DLP are increasingly viewed as low-value areas, with funds redirected to more actionable solutions.

CISOs who have successfully aligned with business functions credit early and frequent engagement. Instead of positioning security as an obstacle, they speak in terms of enablement, impact on revenue, and customer impact. Security teams are embedding themselves into product planning, go-to-market reviews, and executive forecasting meetings. This proactive posture helps CISOs gain influence and ensures their initiatives are well understood across the enterprise.

Some security leaders are also rethinking how they communicate risk to senior stakeholders. Rather than abstract technical metrics, they're translating risks into business language: lost revenue, brand erosion, customer churn. Dashboards are being revamped to focus on KPIs that boards and executives care about, such as time to detect/respond, exposure coverage, and recovery readiness.

THREATS EVOLVING FASTER THAN TOOLS

Attackers are adapting quickly, with social engineering and MFA fatigue tactics on the rise. Even with MFA in place, organizations are vulnerable.

Meanwhile, secure development is underfunded, leaving APIs and modern applications exposed. CISOs express fatigue around overly complex detection platforms like EDR/NDR, which are often noisy and difficult to maintain.

Third-party and supply chain risk remains a common concern, with visibility and control still lagging behind other domains.

To respond more effectively, CISOs are expanding the scope of threat modeling and red teaming. They're conducting simulated phishing campaigns that account for MFA push fatigue. They're investing in API inventory and runtime protection. And they're demanding tighter contract clauses and more frequent attestations from third-party vendors.

There's also a growing recognition that “checkbox” security simply doesn't hold up against dynamic threats. More security leaders are leaning into behavior analytics, identity-contextual alerts, and platform-driven response strategies.

CULTURE, AWARENESS, AND LEADERSHIP

CISO success increasingly depends on communication and education, not just technology. Boards are more engaged than ever, yet many still need better cyber literacy.

CISOs stress that progress and true understanding in cybersecurity isn't linear. It requires consistent effort, clear communication, and support across departments.

Behavioral training is also under scrutiny. Phishing simulations are being re-evaluated in favor of more immersive, behavior-focused learning.

> “One of the most undervalued security areas is training and awareness.”
>
> – Rich Marcus, CISO, AuditBoard

CISOs are investing in ambassador programs, peer-to-peer education, and customized content for different business units. These initiatives are helping shift security from a compliance checkbox to a shared cultural value. When successful, this creates a virtuous cycle: better decision-making, fewer incidents, and more engaged employees.

LOOKING AHEAD

As 2025 unfolds, the role of the CISO will only grow more strategic, with success increasingly defined by collaboration, clarity, and cultural alignment. Organizations that embrace cybersecurity as a business enabler, not a blocker, will emerge stronger, more trusted, and better prepared for the decade ahead.

The most effective CISOs are those who look beyond technology alone. They understand that building trust, shaping culture, and forging partnerships across the business are just as critical as managing risk. In the end, cybersecurity is not just about preventing breaches, it's about enabling resilient, adaptable, and forward-looking enterprises.

PROFILES IN *Confidence*

CASSIE CROSSLEY

VP SUPPLY CHAIN SECURITY
Schneider Electric

Global Headquarters: Rueil-Malmaison, France

Employees: 150,000+

Annual Revenue: $41.2 Billion

BRIDGING CODE AND CONVERSATION

When Cassie Crossley began her career decades ago as a software developer, it quickly became clear that while she loved technology, sitting in silence to write lines of code wasn't her calling. "I'm an extrovert," she says with a laugh. "Back then, project managers didn't exist. It was just, 'Here's the dev manager, now go code.' I couldn't sit still long enough."

That restless energy and need to connect with people would become a defining thread in her career, weaving together deep technical expertise with an intuitive grasp of change management, governance, and strategic thinking. Today, as Vice President of Supply Chain Security at Schneider Electric, a multinational specializing in energy management and industrial automation, Cassie is leading global efforts to secure both hardware and software supply chains.

She's spent nearly 15 years at the company, moving through six different roles that reflect her hunger for challenge and transformation. "When I get bored, I switch gears," she says. "I've always been drawn to complex problems, especially at the intersection of technology and people."

A FOUNDATION IN TECH AND PEOPLE

Her journey into cybersecurity was not a straight line. After leaving software development, she found her voice at Lotus, working in technical support and documentation, Cassie says, "I loved being on the product side, talking to users, improving how things worked."

However, Cassie's first exposure to security came in the 1990s working at McAfee. "We didn't call it cybersecurity then. It was just virus scanning software," she recalls. From there, she moved into project and program management, eventually leading multi-million-dollar initiatives.

At Schneider Electric, she started as a Program Management Office Director and later transitioned into cyber governance, writing the company's IT cybersecurity policies and launching a 'crown jewels' initiative focused on protecting priority applications and data. "This was before CISOs were common in big companies," she explains. "A lot of the early CISOs came from network engineering. I came from governance, change management, and a desire to understand systems holistically."

ARCHITECTING SECURITY FROM THE INSIDE OUT

Six years ago, she shifted her focus from internal IT to product security. In a company with 14,000 R&D employees and dozens of product lines, her team implemented Secure by Design principles, developed secure development lifecycle processes, and curated a training catalog hundreds of hours deep.

Then came the pivotal merger of two security teams, IT and product, which led Cassie to take on her current role: heading global supply chain security. "We're selling into critical infrastructure and governments around the world," she says. "It's not just about the software you're building. It's about where the hardware comes from and how everything is integrated."

Her work now spans continents and disciplines, engaging with regulators from countries like Australia and Singapore, helping define global standards for software and hardware transparency. She worked closely with NIST on its Cybersecurity Framework 2.0, helped shape the CISA Secure Software Development Attestation Form, became a leader in the software bill of materials (SBOM) movement, and has helped governments define IoT labeling baselines.

SILENT RISKS IN THE SUPPLY CHAIN

When asked what security risk is quietly growing in importance, Cassie doesn't hesitate: "Supply chain security. We've heard about it, but the deeper issue is traceability. Most of the chips in our devices aren't high-end AI chips. They're simple processors made years ago, often with embedded firmware from third or fourth-party vendors. And they're everywhere in cars, buildings, and power systems."

This, she says, creates a ticking clock around product longevity. "We've gotten used to disposability, but that doesn't work when digital components are embedded in physical products. You can't just replace a car every five years. What happens when a chip manufacturer goes out of business? Who maintains that firmware?"

Cassie believes this is a problem few consumers and too few executives fully understand.

BOARDROOMS AND BLIND SPOTS

That disconnect extends to the C-suite. "Boards know how to assess a company's financials and external cyber hygiene," Cassie explains. "But when it comes to product development, especially in large companies with hundreds of dev teams, there's no visibility. One team might follow secure architecture principles. Another might not."

Cassie has seen countless third-party security assessments filled out, with companies offering vague reassurances at the global level. "We'd say, 'We do this process globally, but if you want product-level details, let us know.' Nobody ever came back to ask."

She argues that boards need to take a much more active role in understanding digital dependency and resilience. "What happens if Microsoft Teams or Outlook goes down for a week? If your supplier's supplier was using CrowdStrike during the failure? Boards aren't asking those questions. They don't know what's under the hood."

BUILDING RESILIENCE BEFORE IT'S TOO LATE

Cassie is adamant: cybersecurity needs to be embedded across the business, from policy to product, and from governance to grassroots development. She views supply chain not as a checklist, but as a living ecosystem of hardware, software, and global regulation.

Her philosophy? "Ask what you can't live without for a week. Prioritize from there."

With her background in both communication and technology, Cassie is uniquely positioned to navigate this evolving terrain. She may have left software development behind, but she never stopped building, only now, she's architecting the security of the future.

DAN BOWDEN

GLOBAL BUSINESS CISO
Marsh McLennan (MMC)

Headquarters: New York, NY

Employees: 90,000+

Annual Revenue: $24.5 Billion

PROFILES IN *Confidence*

Dan Bowden, Global Business CISO of Marsh McLennan (MMC), doesn't merely run a security program, he stewards a culture. In an era where cyber risk can cripple operations in minutes, Dan's mandate extends well beyond traditional IT parameters. For him, cybersecurity is less a department concern, and much more a global imperative. This global mindset extends throughout the organization and to MMC's valued clients and suppliers.

THE CULTURE OF VIGILANCE

At MMC, cybersecurity isn't bolted on, it's built in. Dan coordinates with key partners to ensure that information security is not only a technical concern but a foundational part of how the business operates. "Security needs to be like your health," he explains. "It's not just something you address when you're sick; it has to be maintained and managed constantly."

His approach emphasizes enablement rather than obstruction. Dan believes that when security is seen as a collaborator, not a roadblock, it's more likely to be embraced across teams. That philosophy has helped MMC align security operations with business priorities, fostering a risk-aware culture where teams are educated, engaged, and empowered to make secure choices in their daily work.

A SEAT AT THE TABLE, ESPECIALLY IN CRISIS

Dan believes that when an incident occurs, boards expectations should be clear. "They don't want hysteria," Dan says. "They want to know that you have a plan, that you're executing against it, and that their trust in you is warranted."

He emphasizes the importance of pre-established relationships across the executive team and with external partners. During an incident, the ability to communicate with transparency, without devolving into panic, is what sets effective leadership apart. Dan notes that breach responses aren't just technical; they're organizational. "You have to show that you can lead a team under pressure, keep the narrative factual, and keep business leaders in the loop without overwhelming them."

OVERVALUED TOOLS, UNDERVALUED STRATEGIES

In a landscape overflowing with technology vendors and hyped solutions, Dan offers a grounded perspective on what's truly valuable in a security program, and what's not.

"There's an overvaluation of the next shiny tool, especially in endpoint or network security," he explains. "It's easy to get excited about a new platform promising AI-based threat detection, but often, organizations haven't fully implemented or optimized the tools they already have."

Conversely, he sees fundamental areas like asset management and configuration control as undervalued. "If you don't have a clear picture of what you own, where it's located, and how it's configured, no tool is going to save you," Dan warns. He also underscores the importance of security operations centers (SOCs) and hands-on talent. "Automation is great, but human skillsets still play a critical role, especially when detecting nuanced threats or anomalies."

ARTIFICIAL INTELLIGENCE: PROMISE AND PRUDENCE

AI is changing the security game, but not always in the ways people expect. Dan is measured in his optimism. "AI has incredible potential, especially in pattern recognition and automating repetitive tasks. But it's not magic, and it's not ready to replace critical thinking."

He's cautious about the overselling of AI-driven solutions and stresses the importance of transparency. "You need to know how these models work, what data they're trained on, and how they're making decisions. Otherwise, you're introducing new risks in the name of solving old ones."

For Dan, the real opportunity lies in augmenting, not replacing, human expertise. AI can accelerate analysis and streamline alerts, but judgment and context remain essential. "The future is human + machine, not machine alone."

LESSONS FROM THE BATTLEFIELD

Dan's insights are grounded in experience across multiple industries, geographies, and incidents. He knows what it means to manage a breach, to brief a board in real time, and to rebuild trust after a close call. His leadership philosophy combines pragmatism and empathy: protect the business, support the people, and never stop learning.

"Cybersecurity is never 'done.' The threats evolve, the business evolves, and so must we," he reflects. That evolution demands not only technical acumen but also storytelling, diplomacy, and a deep understanding of organizational dynamics.

THE NEXT CHAPTER

Looking ahead, Dan is focused on strengthening MMC's cloud security posture, refining detection capabilities, and deepening partnerships across the enterprise. He's also committed to mentoring the next generation of cybersecurity leaders, those who can combine technical rigor with business fluency and emotional intelligence.

In a field too often driven by fear, Dan brings a voice of steadiness, clarity, and resolve. His legacy is not just stronger defenses, but a smarter, more resilient organization that sees cybersecurity not as a cost center, but as a core enabler of trust.

HEATHER REED

HEAD OF CYBERSECURITY
Nestlé Purina PetCare North America

Headquarters: St Louis, MO

Employees: 13,000

Annual Revenue: $21 Billion

BRINGING SECURITY TO THE PEOPLE

When Heather Reed took over cybersecurity for Nestlé Purina in the U.S. and Canada, an organization of 13,000 employees, she didn't just want to keep data safe, she wanted to shift an entire culture. With candor and conviction, she has built an incredibly relatable, human-centered cybersecurity program that continues to demonstrate a forward-thinking strategy.

THE CYBERSECURITY AMBASSADOR MODEL

Rather than relying solely on traditional training modules or awareness campaigns, Heather championed a grassroots solution: a cybersecurity ambassador program. "I have cybersecurity ambassadors in every department in the company and in all 27 facilities. I have two programs, one for factories and one for corporate and sales offices."

From senior directors to recent graduates, ambassadors volunteer to carry the cybersecurity message forward. "They're just everyday people, and they're fascinated by cybersecurity."

Heather embeds messaging directly into the company's monthly "floor meetings" where department leaders share company news and updates with employees. "I've inserted a cybersecurity message into that. I only get 75 words, so I train my ambassadors ahead of time so that they'll evangelize from there."

That internal advocacy has made a measurable difference: "You won't find a person on our campus who doesn't know how to report phishing or how to report a stolen device. That wasn't the case when I first took this role."

OVERVALUED AND UNDERVALUED SECURITY TACTICS

Heather is not shy about calling out what she sees as misaligned priorities in the broader security industry. "I think phishing simulations are overvalued," she says. "Mandatory training and simulations have a place. But what's maybe undervalued is making cybersecurity relevant to people in their everyday lives."

She links security to everything from smart home devices to wearable tech: "Cybersecurity is getting up in the morning and talking to Alexa and taking your kids to school where they're logging into devices you don't know about. It runs the gamut… even while you're sleeping and your watch or ring are tracking your sleep. There's a security aspect to everything we do all day long."

CUTTING THROUGH THE CYBER NOISE

One thing Heather would love to see go? The never-ending amount of cybersecurity acronyms that continually flood the market. "I hate acronyms. The acronyms are out of control. Half the time people are sitting in a meeting and they leave not knowing what in the world was just said."

She advocates for clarity and simplicity: "If it means we need to come up with a new word instead of four words that make an acronym, let's do that."

STAYING IN STEP WITH THE BUSINESS

While many CISOs feel outpaced by business transformation, Heather doesn't see that friction at Purina. "If we don't have a business, we don't have a security department," she says. "We are always trying to make sure that we are putting the priority of the business first while doing it securely, and I think they're on pace with each other."

That alignment is essential in an era of increasing complexity and mounting compliance demands. “When I took this role four years ago, we had 37 measures in our security and compliance index and today we have 112.”

LEADING SECURE AI ADOPTION

AI is one of Purina’s key priorities, and security is baked in from the start. “Nestlé as a whole is taking AI very seriously as part of our digital transformation journey,” Heather says. “We’re using our own NesGPT and approved solutions.”

She’s also monitoring how employees interact with generative AI tools. “We put a lot of effort into making sure that people know to not put company data into random tools.”

Not surprisingly, marketing is the trickiest team to tame. “Marketing is the most rogue,” she laughs. “They want to move quickly and be first to market, but as soon as they understand the ‘why’ and the risk, they take it a lot more seriously. It’s the relationships.”

EMPOWERING THROUGH SCARCITY

Heather’s team doesn’t have endless budget or staffing, as with most security programs across almost all industries. Far from it. “In general, I think that the demands on security and compliance are far exceeding the amount of employees that we’re able to have.”

Her ambassador program, in part, was born out of necessity. “I needed help. And what a great way to leverage others within the company.”

And it’s not just effective, it’s deeply meaningful. “They get to put it in their performance plan. I have a graphic designer who doesn’t get to do graphic design anymore in her day job, so she loves to do it. We have people who like to plan events, and it gives people something interesting to do.”

A PLAYBOOK OTHERS CAN FOLLOW

Heather’s model is a compelling example of cybersecurity leadership rooted in empathy, communication, and real-world impact. “It is, I think, the number one thing that has shifted the culture.”

And when it comes to cybersecurity’s place in the business? “We do everything we can to make it so that we’re enabling a secure business.”

JAVED IKBAL

CISO
BRIGHT HORIZONS

Headquarters: Newton, MA

Employees: 33,000

Annual Revenue: $2.7 Billion+

PROFILES IN *Confidence*

PRAGMATIC DEFENDER

Javed Ikbal isn't easily distracted by hype. As Chief Information Security Officer at Bright Horizons, he's seen enough industry fads come and go to know where real risk lives, and it's not always in the next buzzword.

"Everyone's talking about AI threats and post-quantum cryptography," he says. "But we're still losing ground to the basics. Social engineering is still one of the most dangerous threats, and too many people think giving everyone MFA is enough."

With over a decade at Bright Horizons, a global childcare and early education provider, Javed has cultivated a culture of grounded, intelligent cybersecurity, one where risk is managed not through flashy tech, but through thoughtful prioritization, storytelling, and an unshakable sense of fiduciary duty.

THE REAL THREATS ARE HUMAN

Javed places social engineering under a broader umbrella, human-centric vulnerabilities that can't be patched with software. "You can still walk into an office with a clipboard at lunch and find unlocked computers," he notes. "Remote work has actually helped reduce some of that attack surface. But in physical offices, it's still a real issue."

He sees phishing tests as another area where companies may be over-investing without evolving. "The value diminishes with each repeat test. Doing four phishing tests doesn't make you four times more secure than doing one."

What's undervalued, in his view, is application security. "If you have public-facing apps and remote access infrastructure, that's where nation-state actors are going. VPNs are often the weakest link. Once someone's in, they've bypassed your firewalls. Now it's all about lateral movement."

"IT'S MY JOB TO EXPLAIN IT"

Javed's measured approach extends to his executive relationships. "I've been very lucky," he says. "Any time I've brought something to the executive team or board, I've had their full attention and support. But it's not their job to understand this stuff upfront, it's my job to explain it clearly."

His philosophy on budget echoes this clarity. "Security doesn't get a blank check," he says. "Just like the VP of Marketing is held to their targets, I'm held to mine, mine just look different. I treat every dollar like it's coming out of my own pocket."

That mindset extends to resilience. While Bright Horizons doesn't operate critical infrastructure, it has invested heavily in continuity. "We can fully failover our services in less than 24 hours. We do it not because we have to, but to assure our clients and our board that we protect not just confidentiality, but availability."

KEEPING UP WITH THE BUSINESS

The greatest challenge, according to Javed, is scale, specifically, how to match security operations with the velocity of the business. "Companies will hire 100 engineers pushing 10,000 lines of code per day, but the application security team doesn't scale at the same rate."

He dreams of building a formula, something like a security-to-business ratio, to help organizations baseline their security investments. "If you've got millions of lines of code, how many AppSec people should you have? If you've got X number of firewalls, how many network security folks? It's all out there. We just need to model it."

The shift to DevOps and continuous deployment has transformed the game. “We used to do one big release every six months. Now it’s multiple tiny updates per day. But threat actors don’t wait until your next pen test. They’ll attack any time. And most companies are not keeping up.”

PRACTICAL AI AND REALISTIC EXPECTATIONS

Despite industry hand-wringing, Javed sees AI as a tool more than a threat, at least for now. “We use AI in our call centers for summarization and sentiment analysis. We use it in staff scheduling. We’ve blocked general-purpose tools like ChatGPT, but we’ve approved Microsoft Copilot because it has gone through privacy and security vetting.”

When asked if he’s anti-AI, he smiles. “My job would be impossible without it. I’ve been using AI in endpoint detection and response for years, it’s just called machine learning. It’s not about saying yes or no to AI, it’s about using it responsibly.”

TRAINING WITHOUT THE TRAINING

Perhaps the most innovative aspect of Javed’s approach is how he handles security awareness.

When employees report suspicious emails, they get more than an answer, they get thanks. “We tell them, ‘You did the right thing. Now please share this with your colleagues over lunch.’ That way, we avoid boring PowerPoint trainings and instead create hundreds of micro-trainings every month that are casual, conversational, and far more memorable.”

This subtle form of influence reinforces his broader belief: cybersecurity is cultural, not just technical.

THINKING THE UNTHINKABLE

Javed believes the greatest threat is what you haven’t yet imagined. “It’s the ‘unknown unknowns’ that will hurt you. That’s why we have to think about the absurd scenarios. Why wouldn’t someone steal a car if your dealership leaves the keys inside? Just because it hasn’t happened yet doesn’t mean it won’t.”

He references the concept of the “Black Swan”, unpredictable events that shatter assumptions. “We’ve seen vendors dismiss vulnerabilities as too hard to exploit. The next day someone publishes proof of concept. That’s the game we’re in.”

SECURITY THAT STAYS HUMAN

At his core, Javed’s approach is one of humility and pragmatism. He doesn’t claim to have it all figured out, but he knows what matters: explaining risk clearly, treating security like any other accountable business function, and never underestimating the power of simple human behavior.

“If we get breached,” he says, “it’s not about blaming someone. It’s about asking: did we prepare, did we warn, did we prioritize the right things?”

In an industry often dominated by noise, Javed Ikbal’s quiet clarity is a rarity—and perhaps, a blueprint.

JAY LEEK

Managing Partner and Founder
SYN Ventures

Assets Under Management (AUM): $620 Million

32 Active Portfolio & 7 Exits Since Inception

Years in Business: 4

PROFILES IN Confidence

FROM CISO TO VENTURE CAPITAL

Jay leek didn't follow the conventional venture capital playbook. His path began in the trenches of information security, culminating in high-profile CISO roles where he not only protected organizations from risk but also laid the groundwork for innovation. The pivot to venture capital wasn't born of ambition alone, it was driven by opportunity.

"I started becoming a VC without even knowing it back in the early 2000s when I was at Nokia, we had a strategy of partnering with early stage emerging companies to meet the needs of the organization." Jay then spent 10 years partnering with these early stage companies, giving him the groundwork for what would later become a successful VC career.

He then joined Blackstone in 2012 and comments, "Working at Blackstone overseeing security program across 100+ portfolio companies around the world gave me the unique vantage point to identify emerging problems and partner with early-stage founders solving them."

His time at Blackstone catalyzed a new kind of investing model. He has since founded two venture capital firms designed to do more than just fund companies. His work helps build them with deep operational guidance, market insight, and a network forged from decades in the field. Jay is currently running SYN Ventures, a venture capital firm primarily focused on leading Series Seed and A rounds for cybersecurity startup companies around the world.

ADVISING WITH THE OPERATOR'S EDGE

What sets Jay, and all of his partners in SYN Ventures for that matter, apart in the crowded VC landscape is his operator's mentality and security background. He's not a financier first; he's a problem-solver, a strategist, life-time security professional and a builder. For portfolio companies, that means hands-on advice rooted in real-world execution.

"Our value isn't in just writing a check," he explains. "It's in helping companies scale intelligently, make the right hires, align their go-to-market strategy, and avoid common pitfalls."

THE STRATEGY BEHIND THE CAPITAL

Jay's investment thesis is as structured as it is selective. At SYN Ventures, fund strategies are clearly delineated and tailored to their target segments.

Unlike generalist firms, SYN leans heavily into its domain expertise. "We're not generalists. We're cybersecurity-focused with the discipline of being operators," Jay asserts. That perspective informs not just diligence but also post-investment execution, ensuring founders get more than capital, they get seasoned guidance.

READING THE MARKET

Cybersecurity is perpetually evolving, and few read the market with as much clarity as Jay and his team. He sees today's climate as a study in contrasts: inflated valuations in some areas, under appreciated innovation in others.

"Valuations got ahead of themselves over the last few years. Now we're seeing a return to fundamentals," he says. "The companies that can demonstrate efficient growth, real value, and clear differentiation will survive and thrive."

He's particularly bullish on categories that improve operational efficiency and at the same time, he warns against chasing trend cycles without substance. "If you're not solving a real pain point, you're not building a business. You're building a feature."

THE CYBER BATTLEFIELD ISN'T LEVEL

Despite all the innovation, Jay remains deeply pragmatic about the reality on the ground: cyber defense is asymmetric. The attacker only has to win once. That's why he believes cybersecurity must be approached holistically, with companies investing in layers of resilience not silver bullets.

"There's always going to be a weakest link, and you can't plug every hole," he notes. "But you can create an architecture where a breach doesn't become a catastrophe."

For portfolio companies, that mindset influences everything from product design to customer alignment. Jay pushes founders to understand the threat landscape not just as a technical reality but as a business risk and to build solutions accordingly.

THE AI SHIFT: POTENTIAL, PITFALLS, AND PRAGMATISM

Artificial intelligence is perhaps the most significant disruptor Jay has seen in years, but he urges cautious optimism.

"AI will dramatically change cybersecurity on both sides of the fence," he says. "The same tools that help defenders automate response can also help attackers scale exploits."

He's excited about AI's potential in threat detection, data correlation, and identity validation. But he's equally wary of AI-washing the trend of startups slapping "AI" onto their pitch decks without meaningful differentiation.

"It's not enough to say you use AI," he emphasizes. "You need to prove it's delivering outcomes that weren't possible before and doing it in a way that's explainable, trustworthy, and safe."

ADVICE FOR FOUNDERS IN A NEW ERA

Jay isn't a futurist; he's a realist with a clear vision. His advice to founders reflects that balance: understand your customer deeply, build with purpose, and prepare for turbulence.

"Success isn't about riding the wave," he says. "It's about knowing which waves matter and having the right board to ride them."

For the next generation of cybersecurity innovators, Jay is more than an investor. He's a coach, a challenger, and a champion. And as the digital world becomes ever more complex, voices like his will shape not just where capital flows, but where real impact happens.

KEVIN PAIGE

CISO
ConductorOne

Global Headquarters: Portland, OR

Employees: 85

Annual Revenue: Private Company

PROFILES IN *Confidence*

A VISION ROOTED IN OPERATIONAL EXCELLENCE

With over two decades in information technology and cybersecurity, Kevin Paige brings a rare blend of technical depth and business fluency to the CISO role. “I’m a seasoned Information Technology & Security Leader with over 20 years of results,” he says. “I deliver solutions that optimize performance, security, and efficiency for both the private and public sectors.”

From cutting costs and increasing capability to driving enterprise risk mitigation, Kevin sees cybersecurity not as a constraint, but as a lever. “You can’t be just a gatekeeper anymore. You have to align security to broader company goals.”

IDENTITY: THE QUIET RISK NO ONE HAS SOLVED

If there’s one area keeping Kevin up at night, it’s identity. “I think the one that’s quietly growing is identity and access management,” he says. “It’s always been a risk, but it’s always been hard to deal with.”

That complexity has only deepened with the explosion of SaaS platforms, API ecosystem and now AI agents. “We currently see an issue managing human and non-human identities, and now you’re going to see AI agents acting as human users, potentially talking to other AI agents to help solve problems for the users. There’s a continuing trend of more and more identities that need to be understood and managed.”

Despite 25 years of effort, Kevin says legacy identity solutions still fall short. The real opportunity, he says, is to treat identity as both a security control and a productivity enabler. “Usually it’s, ‘Oh no, here comes security.’ But if you can automate identity and access, give people what they need when they need it, and take it away when they don’t, you can increase productivity and make security look like superheroes.”

WHAT THE BOARD STILL DOESN’T GET

Kevin is candid about the gap between board expectations and cybersecurity realities. “I think the biggest issue is ‘when’ to do security. Security is treated as a cost-center that is expected to be responsible for all security issues in a company, with an assumption something can get bolted on afterward to address security issues and risks.”

He bristles at buzzwords like “shift left.” “Security shouldn’t have to shift left. It should already be part of how people build software and products. It should be instinctual.”

The failure to embed security early, especially in emerging technologies like AI, has real consequences. “People are building agents, giving access to all their data, and then someone finds out the CEO’s vacation schedule and salary through a prompt. It’s like, ‘Oh, maybe we shouldn’t have done that.’”

OVERVALUED: VULNERABILITY MANAGEMENT. UNDERVALUED: IDENTITY.

When asked about program areas that organizations misjudge, Kevin doesn’t hesitate. “Vulnerability management is overvalued. We spend so much time tracking every single vulnerability, cradle to grave. It can be a waste of time.”

He’s not minimizing risk, just reframing it. “Only 1% of vulnerabilities actually matter. We should be solving the root problems, like patch management, instead of managing symptoms.”

On the flip side, identity remains woefully underprioritized. “There are still software vendors charging for SSO. Still apps that don’t support MFA. In 2025, that’s unacceptable.”

AI: THE SECURITY INDUSTRY'S NEXT RECKONING

Like many leaders, Kevin is pouring time and energy into the AI wave, but he's doing it with caution. "AI's barely born, especially LLMs. And we don't know where it's going yet."

He sees AI not only as a new threat surface, but as a test of foundational maturity. "We've got agents, vector databases, real-time SaaS integration, what happens when someone gets in the middle and owns everything?"

He's tracking issues from input validation to model hallucination, but the real risk is speed without guardrails. "Everybody wants to go fast. But if you're going fast with no focus or direction, where are you going? You're going nowhere fast."

SINGLE PANE OF GLASS?

Kevin isn't afraid to call out industry clichés, and one in particular draws his ire. "Single pane of glass, that's probably the one I dislike the most," he says. "Even as a metaphor, it doesn't make any sense."

He laughs about how marketing teams pitch it. "We joke: 'Oh, you mean a dashboard?' It's never one pane. And if it is, that's not even good enough for my house anymore, I need double pane."

SECURITY AS INNOVATION, NOT OVERHEAD

Perhaps Kevin's most important message is about perception. "Security can't be a cost center. That mindset is part of the problem."

He draws a parallel to physical safety. "People get in their cars and put on their seatbelts without being told to do so. They expect airbags and anti-lock brakes. So why don't we apply that same thinking to how we build technology?"

For Kevin, the future of cybersecurity is clear: less friction, more trust, and a permanent seat at the table. "Security isn't separate from innovation, it is innovation. And when we build it in from the start, we make everything stronger."

PROFILES IN *Confidence*

KONRAD FELLMANN

CISO
Encore Capital Group

Headquarters: San Diego, CA

Employees: 7,300+

Annual Revenue: $1.5 Billion

A CAREER BUILT ON IMPACT

Konrad Fellmann's career journey began as a Marine Corps officer, working in logistics. He then became an implementation consultant for a product data management software company, coding, and customizing software. However, he soon realized he was interested in different types of responsibilities. "I just got bored, it was too easy, and I needed another challenge." That led to a long consulting career across industries and eventually building a global security program at Cubic before joining Encore Capital Group.

Why the move to Encore Capital Group? "I saw the level of investment they were making in security and that they had a lot of different and interesting security projects going on. It's awesome to be part of that and to help the organization mature." He's energized by the opportunity to accelerate progress: "It's exciting to see how we can continue to grow the security program."

THE PACE OF CHANGE

Konrad stepped into his CISO role at Encore Capital Group with a clear-eyed view of what it takes to modernize cybersecurity programs: understanding risk, staying ahead of emerging threats, and creating a culture of collaboration. "It's an ongoing evolution," he says. "We have to be able to increase with the pace of technology and the threats that are out there."

Konrad acknowledges that while most organizations' business goals tend to remain constant (e.g. increasing efficiency), security must keep up with how those goals are pursued. "We just need to keep pace with the rate of change in technology, regulations and threat actor tactics and what else we need to combat, especially if we're entering another market or changing technology for our core systems."

RISK VERSUS MATURITY

Konrad is pushing his organization to think differently about risk. "Talking about the difference between maturity versus risk, achieving a high level of maturity doesn't necessarily mean you're tackling all of those new threats and risks that are coming out." His message to boards and executives: maturity is not the finish line. It's about aligning controls with emerging risks.

He also challenges the notion of overbuilding: "We don't need to shoot for the Maserati level in each security domain, let's save ourselves some time and effort and take smaller steps that can provide immediate value and risk reduction."

INVESTING WHERE IT COUNTS

In terms of security investments, Konrad is focused on consolidation and efficiency. "As organizations grow and mature over time, they typically collect a variety of disparate tools, so the challenge is how can we reduce those into a fewer number of platforms to drive more effective correlation, efficiency and potential reduction in expense?" He wants fewer solutions doing more work.

One area where he sees a potential to shift priorities across the security industry is identity management. "Identity governance is probably a little overvalued, and where I'd probably focus more is the identity protection space." His reasoning is practical: "You can get a lot more value at a lower cost from identity protection...providing improved, inline protection against identity-based attacks, especially when over 90% of organization are reporting identity-based incidents."

AI, BUZZWORDS, AND BUILDING GUARDRAILS

AI is no longer avoidable, it's operational according to Konrad. He says, "We built a governance process with governance guidelines for how we onboard any new AI related project. The aim is to make risk-informed decisions and avoid "just leveraging everything that exists."

As for security buzzwords, there's one he's ready to retire: "Zero trust gives a false impression. I don't think it's something we still need to use." He's also weary of the acronym avalanche: "I can't get them straight anymore. It's just way too many, especially when it comes to all the various cloud security products."

BUDGET REALITIES AND RESILIENCE

Even with strong investments in cyber programs, Konrad knows there are limits. "No security team at any organization can expect to have unlimited resources. We must work within reasonable constraints." He urges teams to be strategic: "Maybe you need to change some processes, get rid of busy work, consolidate platforms and get to a more manageable place to drive efficiency."

When it comes to resilience, the expectations are different now. "Executives want to have confidence that we can minimize the impact of a potential breach. That we can detect security events quickly and stop that lateral movement."

CULTURE AND COLLABORATION

Security isn't siloed at Encore Capital. "I get to regularly speak with executive management and the board, so security is always top of mind." What stood out to him immediately was the company's formal risk appetite statement: "Understanding the level of risk the organization is willing to take and what their tolerances are around cyber. This helps ensure everyone is on the same page."

He sees his role as collaborative, not controlling: "We're not the department of 'no'. The way I like to operate is you tell me your problem so I can find a solution that helps you do your job better."

PROFILES IN *Confidence*

MATT SHAW

CISO
Southcoast Health

Headquarters: New Bedford, MA

Employees: 8,100

Annual Revenue: $1.5 Billion

Matt Shaw didn't begin his career in cybersecurity, he shares. "I started out in banking, many years ago, basically as a bank teller," he recalls. "I was working as an accounting manager, and the bank was notified they needed to move to a new data processor. With no dedicated IT staff, I saw it as an opportunity and managed the data conversion project." That decision launched a new career in technology.

What began as a foray into IT during a systems migration in the early 2000s evolved into a full-fledged career in security leadership. "In banking, it's very regulated," he explains. "You're dealing with federal examiners, a lot of oversight, and that always kept security top of mind; even in an IT role."

Over time, Matt moved into fully dedicated information security roles, eventually taking on larger responsibilities across financial institutions before transitioning to the healthcare industry. Today, he is the CISO at Southcoast Health, a not-for-profit health system that serves communities across southeastern Massachusetts and Rhode Island as the largest provider of primary and specialty care in the region.

"Going from banking to healthcare was a significant change," he says. "Although the basic concepts are the same, the mission is very different. It took a while to shift from protecting customers' personal information and money to protecting patients' private health data and the systems that care for them."

NAVIGATING THE GRAY AREA OF HEALTHCARE SECURITY

That industry shift revealed stark differences in how cybersecurity is applied. "Banking is very black and white, and rigid in terms of regulation," Matt explains. "Healthcare is more complex, there are more gray areas. Data flows, patient care systems – it's all interconnected."

The complexity of protecting electronic health records and clinical workflows shaped Matt's leadership style. "It's not just about technology and security. You have to build relationships across the organization," he says. "People need to see you as a resource, someone who helps them find solutions that support the business securely."

LEADING WITH RESPECT AND VISION

Matt's leadership philosophy centers on empathy, accessibility and mentorship. "I do tend to lead by example, especially in how I treat people," he says. "Security teams are sometimes seen as blockers to business initiatives. I want my team to be collaborative, supportive and respectful. I want colleagues across the organization to see the security team as a resource, and to reach out with any questions or problems, so we can provide them with secure solutions that support their needs. At the end of the day, we rely on employees' awareness and vigilance to help keep us secure, so we need to maintain good relationships and be seen as a partner."

That also means investing in his team's growth. "We're big proponents of promoting from within. Whether someone's going the technical route, such as an engineer, or into a less technical GRC role, I try to support them and provide career paths that keep them engaged."

He's also hands-on by nature. "Sometimes I'm in the weeds more than I should be," he admits. "But being a smaller team, I think it helps to stay close to the details."

BUILDING A PROGRAM

In recent years, Matt's team has invested heavily in top-tier security tools. Now, the focus is shifting toward optimization. "The next 12 months is all about further leveraging the tools we've implemented, and maturing the program," he says.

He's especially wary of overlapping functionality. "The number of security products available continues to grow very rapidly, as does their functionality. We try to be selective and minimize tool overlap. Making sure we get the most out of our products helps the team be more efficient with fewer dashboards and more focused attention."

The goal: reduce redundancy, tighten integration and ensure engineers aren't spread too thin. Having too many consoles and not enough eyes on them is not efficient and increases the chances something gets missed.

IDENTITY, INTEGRATION AND THE QUIET RISE OF RISK

One of Matt's top concerns is identity. "There's a lot of risk in identities – especially as systems become more integrated," he says. "Conditional access, behavioral analytics – these are must-haves."

With cloud-based platforms like Microsoft 365 becoming ubiquitous, he sees threats increasing. "Office 365 is one of the most phished platforms out there. So, it's about having systems that know the baselines of normal user behavior and alert us when something's off and atypical activity is detected, indicating a user account may be compromised."

He's also focused on increasing awareness of how attackers evolve. "Although phishing has been around for many years, it continues to be a huge risk. Attackers are using AI to enhance their efforts and look more credible, and they are constantly evolving their tactics to improve their chances of success. Keeping folks aware of emerging threats and tactics is an important part of helping to keep our employees safe."

AWARENESS OVER ASSUMPTIONS

Matt's team is moving toward more targeted, role-specific awareness training. "Someone in accounts payable is going to get different threats than someone in HR. So why give them the same training and phishing tests?"

That tailored approach is designed to reduce fatigue and increase engagement. "It's about awareness and training opportunities; it's not about punishing people for clicking on a phishing test. The goal is to help them understand the risks and why vigilance is important."

In healthcare, he adds, the stakes are too high, and one-size-fits-all approaches aren't as effective. "There are certain groups of staff who may use email only once a day, and they're just as likely to be targeted. So, we try and layer controls to limit exposure and minimize impacts if they fall victim to a phishing email."

THE HIRING DILEMMA: SKILLS AND SOFT SKILLS

Matt acknowledges the industry-wide challenge of hiring. "The biggest challenge for us is people. It's always hard getting enough of them and finding the right mix of experience and soft skills."

He's looking for a balance. "Having the technical skills is essential, but our team members also need to collaborate and support the employee population. Within our department, everyone is employee-facing, so we can't afford to have someone with poor interpersonal skills. It's not good for the organization, the team, or how we want to be perceived by the organization."

Certifications are also part of his team's DNA. "When I started, I was the only one on the team with industry certs. Now, almost everyone on the team has at least one. Although certs are not the ultimate determinant of someone's tech skills, they demonstrate an understanding of specific security concepts, and help keep employees in sync with industry changes due to the need for Continuing Professional Education (CPE). We support them in getting certified and keeping up with CPEs."

ON BUZZWORDS AND BURNOUT

Ask Matt which buzzword he'd like to retire, and his answer is simple: AI. "With AI in the forefront these days, every product seems to tout AI functionality, but it's often older technology rebranded for today's marketplace and not really AI. It's overused and often misused."

And while AI certainly does play an increasingly important role in security and technology, he warns against overreliance on hype. "With everything claiming to be AI, it's important to make sure you know what you're getting, that it meets your needs, and that it works as advertised."

INVESTING IN THE FUTURE – PEOPLE FIRST

For Matt, building a strong program isn't just about the right tools, it's about people. "At the end of the day, we're a support organization for Southcoast Health. We're here to protect the organization, and that starts with helping people do their jobs securely."

He stays current through a steady diet of news feeds, peer groups and vendor conversations. "Our security partners are great resources, and we value our relationships with them; they see a broad landscape. We're in constant dialogue, not just when we're looking to buy something."

In a complex, fast-moving field, Matt keeps his focus simple: "Be collaborative. Be curious. Be clear. That's how you move security forward."

PROFILES IN *Confidence*

MICHAEL COATES

Founding Partner
Seven Hill Ventures

Active Portfolio (since inception): 18

Distributions to Paid-In (DPI): 2.36

Total Value to Paid-In Capital (TVPI): 3.78

FROM THE FRONTLINES TO THE FOUNDER'S CHAIR

Michael Coates has spent his career leading from the front, a large milestone was serving as Twitter's inaugural Chief Information Security Officer. "It was fascinating," he says of his Twitter tenure. "Blazing the trail of what that means in a company, why they have me there, what the role needs to accomplish was really rewarding."

But Coates wasn't content with corporate comfort. "I left to start my own company. I co-founded Altitude Networks, focused on data security and cloud collaboration platforms like Microsoft 365 and Google Workspace. It was born out of a need I felt as a CISO and I found that nobody had built a solution yet."

Like many in the Bay Area, he leaned into entrepreneurship. "The natural thing to do in San Francisco is quit your job and form a company." Altitude's product gained traction across industries and eventually exited through acquisition, where Coates stayed on for three years, wearing multiple hats. "I worked as Chief Information Security Officer, VP of Engineering, COO. I've found that if there are problems, I charge towards them myself."

Parallel to building companies, Coates ran a side investment fund, backing early-stage cybersecurity organizations. "I wrote large checks for companies founded by people in my network," he says. "I had a great network and an eye for what cybersecurity products the market needs."

His track record speaks volumes. One early investment was acquired by Palo Alto Networks for $300 million in just four years. "Of my small portfolio, I had a large number of markups."

Today, Coates is all in. He's launched Seven Hill Ventures, a full-time venture fund investing exclusively in early-stage cybersecurity companies in the U.S. and Israel. "To invest at the very beginning in cybersecurity, a highly technical field, you have to know it inside and out," he says. "You have to understand the technology, the buyer, the priorities, what a good founder is. And the number of people that have the background to do that are pretty small."

LEADING FROM THE TRENCHES

Leadership, for Michael, is rooted in visibility and trust. "The leaders I admired most were the ones who weren't afraid to be in the trenches," he said. "They understood what was really happening on the ground and weren't sitting in an ivory tower making decisions in a vacuum."

That ethos shapes how he builds teams and mentors others. Whether helping startups shape their first security strategy or advising enterprise CISOs, his guidance is laced with pragmatism, not panic.

BUILDING FOR TRUST

While many investors focus on market opportunity or disruptive technology, Michael zeroes in on something more foundational, trust. In cybersecurity, it's not a bonus. It's the barrier to entry.

"My role is to maximize return, fundamentally," Coates explains. "To do that, I help align founders to what helps their company grow. And at the earliest stages, the most important things are velocity on a problem that matters." That means finding real pain points and building solutions that directly serve the buyer's needs, not abstract use cases or theoretical advantages.

For security startups, those buyers are often other CISOs, some of the most discerning and skeptical customers in any industry. "You're not just selling to a business," Michael says. "You're selling to people whose job is literally to not trust you."

That's why Michael pushes founders to reduce friction wherever possible. "A lot of my early-stage guidance is about removing unnecessary barriers for customers. For example, I always recommend pursuing a SOC 2 certification early, not because it makes you secure overnight, but because it shows your buyer you take trust seriously."

He adds that timing matters: "It's a cheat code. If you do it when you're four people, it's a lot easier than when you're 40. Building those practices early creates muscle memory. And when a buyer asks for your SOC 2 report, you don't have to say, 'We're working on it.' You have it."

Beyond certifications, Michael stresses the importance of how startups present their products. "Buyers expect a certain baseline of security capabilities now, things like SAML integration, two-factor authentication, and role-based access controls. These aren't 'premium features' anymore. If you charge extra for basic identity controls, you're signaling to your buyer that you don't understand them."

Michael considers this part of a broader conversation around product-led security. "You don't need to be a 100-person company to get this right. Even a seed-stage team can build thoughtful security into the product experience. That's what builds trust, and trust is what closes deals."

This mindset shapes how he evaluates founders, too. "I gravitate toward technical founders who've felt the pain firsthand. That's the DNA you want. They're not just chasing a market, they're solving a real problem in a way that's usable and scalable."

In a space crowded with acronyms and buzzwords, Michael sees simplicity and transparency as differentiators. "Too many companies try to mask immaturity with language. But smart buyers see through that. Just be honest about what your product does, what it protects, and how you'll grow."

Ultimately, Michael believes that early-stage security decisions, when made intentionally, aren't just technical. They're strategic. "Security can be a lever for growth if you do it right. It's not just about mitigating risk. It's about creating confidence in your product, your team, and your future."

THE SECURITY FOUNDER'S MINDSET

Co-founding Altitude Networks was a major inflection point. It wasn't just about building a tool to solve a problem, it was about designing a solution that users could understand, deploy, and trust. "As a founder, you don't just wear the product hat. You're wearing the marketing hat, the sales hat, the trust hat," Michael explained. That multifaceted experience shapes how he advises other founders today.

He's candid about the pressures that come with building in security, especially when selling to other CISOs. "Security buyers are inherently skeptical. If you don't have your own house in order with secure coding practices, clear messaging, solid customer support, they'll see right through you."

MENTORSHIP, MOTIVATION, AND MAKING A DIFFERENCE

For Michael, cybersecurity is more than a job, it's a mission. He's especially passionate about mentoring the next generation of security professionals, encouraging them to stay curious and resist the urge to chase flashy titles. "If you focus on learning and growth, the opportunities will come," he advises.

He also encourages others to embrace failure as part of the process. "I've had projects that didn't work out. I've made decisions that, in hindsight, weren't ideal. But each one taught me something. That's how you grow."

Michael's blend of technical depth, business acumen, and people-first leadership continues to influence the industry. Whether guiding a startup or advising a Fortune 500, his approach remains the same: "Security isn't about saying no. It's about finding a way to say yes, safely."

MICHAEL NEWBORN

CISO
Navy Federal Credit Union

Headquarters: Vienna, VI

Employees: 25,100

Annual Revenue: $12.5 Billion

PROFILES IN *Confidence*

Mike Newborn currently serves as the Chief Information Security Officer (CISO) at Navy Federal Credit Union, where he brings more than 26 years of cybersecurity experience to the world's largest credit union. His career is defined by a balance of deep technical expertise and a mission-driven passion for helping people manage technology and risk.

Before joining Navy Federal, Newborn served as CISO for McKinsey Digital Labs and held the title of Associate Partner at McKinsey & Company. In that role, he advised many of the world's largest corporations on how to build and execute enterprise-grade cybersecurity programs.

Earlier in his career, he led critical security functions at Bloomberg, and at VeriSign, where he oversaw the protection of global infrastructure including the Internet's DNS, PKI, and SS7 systems, core technologies that underpin global communications and digital trust.

His operational depth spans virtually every aspect of security: network defense, application security, vulnerability management, cloud architecture, incident response, and GRC. Colleagues describe him not just as a cybersecurity expert, but as a leader who scales teams and systems with equal effectiveness.

SECURITY IN THE DNA

Currently, Mike's focus is building a proactive, business-aligned security strategy that doesn't slow innovation. He says, "If security becomes a blocker, you've lost the room."

He believes the key is to position security as a strategic enabler. "You can't just say no. You have to explain why, offer a path forward, and stay connected to business outcomes. That's how you get traction."

Mike credits much of his success to building trust across the organization. "You've got to show people that you understand their world. What makes sales successful? What matters to engineering? If you come in with that empathy, they'll start to see you as a partner, not a police officer."

TRAINING THE BUSINESS TO THINK LIKE SECURITY

Culture, Mike believes, is where security wins or loses. "If your people don't understand the why behind security, they'll find a way around it."

He's focused on building security awareness programs that are role-specific and relevant. "It's not enough to say, 'don't click on phishing emails.' You've got to connect the training to the actual work people do. Give developers secure coding patterns. Teach finance teams how wire fraud happens. That's how it sticks."

He also points out that top-down leadership is essential. "Executives set the tone. If they care about security, others will too. But if it's just lip service, it dies on the vine."

WHAT BOARDS REALLY WANT TO KNOW

Mike is no stranger to board-level conversations and stresses the importance of transparency. "When I talk to boards, they don't want a technical deep dive. They want to know: Are we prepared? Can we detect and respond? Are we resilient if something goes wrong?"

He believes fear-based messaging is a mistake. "Boards don't want to be scared, they want to be informed. It's our job to translate the risk into language they understand and show them the business impact."

GETTING THE FUNDAMENTALS RIGHT

While industry headlines often chase the latest zero-day or nation-state threat, Mike remains grounded in the basics. "You can have the flashiest tools in the world, but if your patch management is broken, you're wide open."

He's passionate about prioritizing hygiene: "Identity, access, asset management, these are table stakes. But they're hard. And if you don't get them right, everything else is just noise."

AI AND THE SECURITY STACK

Like many CISOs, Mike is navigating the fast-evolving world of AI. But he cautions against overhype. "AI can be a force multiplier, but it's not a silver bullet. You still need governance, human oversight, and strong data hygiene."

He's particularly focused on how employees use generative AI tools. "We've had to put guardrails in place. It's about balancing innovation with risk. You want people to use the tools, but safely."

LOOKING AHEAD: WHAT'S NEXT FOR CYBERSECURITY LEADERS

Mike sees the CISO role continuing to evolve from technical manager to business strategist. "Security is no longer just about firewalls and alerts. It's about brand trust, market differentiation, and resilience."

For those entering the field, his advice is clear: "Focus on the fundamentals, build relationships, and never stop learning. The landscape changes fast, but the principles stay the same."

RICH MARCUS

CISO
AuditBoard

Headquarters: Cerritos, CA

Employees: 800+

Total Number of Customers: 2,300+
More than 50 percent of the Fortune 500, and 7 of the Fortune 10, use AuditBoard's modern connected risk platform

LEADING FROM THE MIDDLE: RICH MARCUS' VISION FOR CYBERSECURITY AT AUDITBOARD

For Rich Marcus, cybersecurity is as much about mindset as it is about tools. As CISO of AuditBoard, he sees his role not only as a technical leader but also as a bridge between business, operations, and risk.

"I've always liked working in the middle of things," Rich says. "I like building connections across an organization. That's really where the CISO role lives, at the intersection of business and security."

That position, he says, requires empathy and communication. "You must understand what different teams care about. Legal might be thinking about contracts, engineering might be thinking about velocity. My job is to align security with those priorities without slowing them down."

SECURITY AT A GROWING SAAS COMPANY

AuditBoard is a SaaS-based risk management platform trusted by some of the most security- and compliance-conscious organizations. "We're a company that sells to audit, risk, and compliance professionals. So, we don't get a lot of leeway if we're not doing security well," Rich says.

Operating at that level means security must be built in, not bolted on. "When you're a SaaS company, your software is your product. If the product isn't secure, your entire business is at risk. Our customers expect that we meet the bar and increasingly, that we help raise it."

That also means that demonstrating compliance isn't enough. "Customers want to see evidence. They want to know how you manage data, how you control access, what happens in an incident. It's not just check-the-box anymore. It's operational."

ENABLING GROWTH WITHOUT SLOWING IT DOWN

Security programs at scale often struggle with speed, but Rich is committed to enabling, not obstructing, growth. "I don't want to be the reason a product launch is delayed. Security can't be an afterthought, but it also can't be a roadblock."

That means deep partnerships with product and engineering. "We work alongside those teams, not above them. When we're in planning meetings, roadmap discussions, sprint reviews, we're contributing value, not just saying 'no.'"

He also emphasizes automation and tooling as enablers. "Manual processes don't scale. If you can't automate access reviews, patch management, or alerting, you'll get buried. So, we invest in systems that reduce friction."

RETHINKING THE RISK CONVERSATION

For Rich, real cybersecurity maturity means separating hype from substance. "There's a lot of noise in this space. But if you look at the root cause of most breaches, it's the basics: exposed credentials, unpatched systems, excessive privileges."

He focuses his team on strengthening these fundamentals. "We're ruthless about identity management. We segment access. We monitor privilege escalation. These aren't glamorous, but they work."

He also critiques the overuse of fear-based messaging. "I don't need to scare people into caring about security. I need to make it relevant to their job. If someone in marketing understands how phishing impacts brand trust, they'll be more invested."

AI: AN OPPORTUNITY WITH GUARDRAILS

AI presents both promise and risk. Rich approaches it pragmatically. "Everyone wants to leverage AI, and we do too, but we have to be deliberate. We have policies in place for generative AI use, and we've defined what data can and can't be used."

Internal governance is key. "We don't ban tools just to ban them. We evaluate risk, define acceptable use, and educate users. That builds trust and ultimately leads to safer adoption."

He's also watching the AI space evolve. "AI will change how security teams operate, from detection to response. But it won't replace fundamentals. We still need smart people making good decisions."

A BOARD THAT GETS IT

At AuditBoard, Marcus has something many CISOs envy: engaged, informed leadership. "Our board understands that security is existential. They ask smart questions. They're not just looking for dashboards, they want context."

That relationship is built on transparency. "We don't sugarcoat things. If there's a risk, we say so. And if we don't have something fully solved yet, we say that too. That openness builds credibility."

He regularly shares not just performance metrics, but lessons learned. "If we had a near miss or a false positive, we talk about it. That shows we're not just measuring success, we are demonstrating resilience."

THE CISO'S REAL JOB: INFLUENCE

Technical skills are critical, but for Rich, influence is what defines an effective CISO. "If I can't convince people why something matters, it doesn't get done. Influence is the lever."

He's deliberate about tailoring his message. "When I talk to engineers, I get technical. When I talk to executives, I talk about business impact. You must speak the language of your audience."

That adaptability helps drive alignment. "We want security to be a shared responsibility. That means making it part of how the company operates, not just something the security team owns."

RESILIENCE OVER PERFECTION

Ultimately, Marcus doesn't aim for zero risk, he aims for resilience. "We're not naïve. We know we can't stop every threat. But we can design systems that recover fast, that limit blast radius, that learn and improve."

That mindset informs everything from architecture to incident response. "We train for failure. We practice scenarios. We ask: what if this breaks? How do we contain it? How do we learn from it?"

For Rich, it's this operational rigor, not flashy tools or marketing buzzwords, that will define the next generation of great security programs. "Resilience isn't reactive. It's built in. And that's what we're focused on every day."

RICK ORLOFF

CISO
Pure Storage

Headquarters: Santa Clara, CA

Employees: 6,000

Annual Revenue: $1.5 Billion

PROFILES IN *Confidence*

UNDERSTANDING THE RISK LANDSCAPE

Rick Orloff is currently the CISO at Pure Storage, and brings over 20 years of experience as a technical and business enabler, bridging gaps and bolstering security programs. When Rick steps into a boardroom, he brings more than expertise, he brings a reality check. A veteran of cybersecurity leadership roles at Apple and other organizations throughout Silicon Valley, Rick has built a career around confronting misconceptions about digital risk. “Most people believe that we have controls in place and they’re strong enough, and the truth is, they’re not,” he warns.

According to Rick, many executives view cyber threats through an outdated lens. “We’re dealing with a different threat model today.” The core issue? “Somebody got access to something they shouldn’t have. So what is the root problem?.” He emphasizes that the focus must shift from headline-making breaches to the basic principles of access control. “The vast majority of successful attacks are identity based.”

THE IDENTITY AND ACCESS CRISIS

For Rick, a lot begins and ends with identity. “You must govern access and identities,” he says. “And if you don’t have a governance program, you’re likely going to be breached or already have been.”

Identity is no longer a background function, it’s the foundation. “If you know how to govern identity and access, you’re probably halfway there in terms of protecting your organization.” He frequently sees companies investing heavily in security tools without understanding how poorly governed identities are leaving the door wide open. “Even if you have an identity program, if it’s not governed and if it’s not properly supervised and audited, then it’s probably a vulnerability.”

The challenge, he adds, is scale. “You have to know what vendors you have, what access they have, and who manages them. Most companies can’t answer those questions.”

CYBERSECURITY IN THE BOARDROOM

Rick believes boards of directors must play an active role in cybersecurity oversight, but that doesn’t mean they need to become technologists. Instead, he encourages them to ask focused questions.

He urges board members to go deeper. “Ask the same question in three or four different ways. If you get a different answer, you have a problem.” Clarity and consistency are key. “You want to create a culture where cybersecurity is not separate from the business, it is engrained with the business.”

He also emphasizes the importance of aligning cyber risk with business risk. “Every business function has cyber implications, and every board decision has cyber consequences. So, it’s not just an IT problem, it’s a business resilience conversation.”

RETHINKING SECURITY INVESTMENTS

Despite the flood of new security tools hitting the market, Rick cautions against blind spending. “I think the most overvalued security program area is SIEM,” he says. “People have over-rotated and over-invested without properly thinking about what outcome they want.”

Instead, he advises a more disciplined, business-first approach: “What are the crown jewels? How do we protect those? How do we understand how they’re being used and accessed?”

His message: don’t buy the tool until you understand the problem. “People buy all this tech, but don’t know how to operationalize it. It’s shelfware.”

AVOIDING THE COMPLIANCE TRAP

Rick has seen too many security programs driven more by audit requirements than actual risk. “Is the program driven by compliance, or is it driven by risk?” he challenges. “Because those are two very different things.”

Compliance may check boxes, but it doesn’t prevent breaches. “You can be 100% compliant and still 0% secure,” he says. “The objective should be business continuity and risk mitigation, not passing an audit.”

He emphasizes that success comes from prioritizing outcome-based thinking: “What business function are we enabling or protecting with this investment?”

SIMPLIFYING SECURITY FOR THE BUSINESS

One of Rick’s core goals is to demystify cybersecurity for non-technical leaders. “Cyber is not about complexity,” he says. “It’s about understanding your data, understanding your identities, and controlling access.”

He believes the best CISOs are those who speak the language of business. “I want the board to understand why we’re doing what we’re doing and what the outcomes should be. If they can’t repeat what you just said back to you, you’re not communicating effectively.”

Rick also coaches CISOs to align their programs with corporate strategy. “If you can show how your cyber investments support growth, innovation, and resilience, then you’re not just a security leader, you’re a business leader.”

FROM PRACTITIONER TO ADVISOR

Rick’s influence today goes beyond operational leadership, he’s a trusted advisor to boards, executives, and emerging cybersecurity leaders. He sees himself as both an educator and a challenger. “Occasionally my job is to make people uncomfortable in a constructive way,” he says. “Because discomfort leads to awareness, and awareness leads to change.”

For organizations looking to future-proof their cybersecurity posture, Rick’s advice is clear and grounded in experience: govern access, ask the right questions, and stay focused on business outcomes.

“If you can’t tell me who has access to what, why they have it, and how it’s being used, then you’re not secure. And no amount of technology will fix that.”

VIOLET SULLIVAN

AVP, CYBER SOLUTIONS TEAM LEADER

Crum & Forster

Global Headquarters: Morristown, NJ

Employees: 2,600

THE CALM IN THE CYBERSTORM

Violet Sullivan is currently the Associate Vice President, Cyber Solutions Team Leader at Crum & Forster. She says, "My job is to be the calm in the chaos. I'm the person that brings a little bit of structure and maybe even a little bit of levity when it's a very stressful time for a company."

That unique ability to lead with clarity during cyber incidents where seconds matter and stress runs high has made her a trusted partner across all cyber response needs. Whether working alongside internal teams or clients navigating a breach, Violet thrives on creating confidence where there's often confusion. "There's something really rewarding about being in the trenches with people when they're having their worst day," she says. "And being the person who says, 'Hey, we've got this.' That's why I love what I do."

TRANSLATING AND COMMUNICATING EFFECTIVELY

Today, Violet wears many hats. "I'm a licensed attorney. I have my MBA. I teach at a law school. I speak at national conferences and am very active in the thought leadership space around cyber preparedness," she explains. Her versatility allows her to operate in technical, legal, and executive circles, often acting as the translator between them.

"If I'm on a call with a bunch of engineers, I'm not going to give them a legal memo. If I'm on a call with the GC, I'm not giving them the technical jargon," she says. "I'm the translator."

CYBER SIMULATIONS: TRAINING FOR THE WORST DAY

Violet is passionate about proactive preparation, especially breach simulations and tabletop exercises. "When it comes to simulations, that's where I shine," she says. "I love being in front of people and making them squirm just a little bit so that we can have a moment of realization, 'this is not our strongest area', and then build confidence."

Her approach is rooted in the belief that crisis performance isn't innate, it's practiced. "We all think we're going to rise to the occasion," she explains, "but in a crisis, you fall to your level of training. So, if you've never practiced a breach response, if you've never sat in that seat, if you've never led the call, you're not going to just miraculously be great at it."

In those exercises, she focuses on human readiness, not just technical responses. "Cybersecurity is not a technical issue," she says. "It's a leadership issue. It's a communication issue. It's a process issue."

EMPOWERMENT, NOT FEAR

Violet's work centers on empowering teams with confidence, not burdening them with anxiety. "It's not about scaring people. I want to empower people," she says. "I want them to feel like, 'Yeah, I can handle this. I've seen it before. I've practiced it.'"

Her ability to lead with empathy is a signature strength. "I like people. I'm a communicator more than anything else. I just happen to have legal and technical experience," she says. It's this human-centered mindset that makes Violet a trusted advisor before, during, and after a cyber crisis.

THE EVOLVING ROLE OF AI IN CYBERSECURITY

Among the most exciting, and complicated, areas Violet is watching closely is artificial intelligence. "Everybody's trying to figure out what AI means and what it's going to do," she says. "But it's a little bit like ChatGPT, right? It's only as good as the questions that you ask."

She sees immense potential in AI but is also grounded in its limitations. “You have to know how to ask the right questions and what to do with the answers,” she explains. “That’s how I view AI in general. It’s going to be great, but it still needs humans to use it well.”

AI also poses new challenges in how teams prepare for and respond to threats. “We’re going to have to be careful,” she says. “AI will make some things better, and some things worse. We just have to train people to be smart and curious and thoughtful about how we use it.”

Her focus is less on replacing human insight and more on enhancing it. “You can’t automate good leadership,” she notes. “And you can’t outsource accountability in a crisis.”

INSIDE CRUM & FORSTER’S APPROACH TO RISK

At Crum & Forster, Violet plays a key role not only in response but also in strategic preparedness. “I work closely with breach response vendors, underwriting teams, and claims counsel to identify and onboard partnerships, evaluate vendor performance, and refine internal incident response procedures,” she says. Her work touches everything from policyholder support to internal simulation programs.

On the insurance side, she sees how companies often underestimate their exposure. “Sometimes we might offer free loss mitigation or preventative pre-breach services,” she explains, “but they treat it like insurance. It’s just there if something bad happens.” That mentality, she argues, is risky. “If people are only thinking about insurance in terms of financial coverage, they’re missing the point. It should also be about support, response, and readiness.”

LEADERSHIP IN THE FACE OF UNCERTAINTY

For Violet, effective crisis leadership starts well before the incident. “You have to practice being decisive,” she says. “You have to practice being calm. That’s why I push these exercises so hard. You’re not going to just magically lead well if you’ve never been tested.”

Her philosophy is simple but powerful: be ready, be human, and be adaptable. Whether facing down a sophisticated ransomware attack or navigating the complexities of emerging AI threats, Violet returns to her core purpose. “My job,” she says, “is to be the calm in the chaos.”

The Transformative Role of Venture Capital and Private Equity in Cybersecurity Startup Innovation

By Katie Haug

In the ever-evolving world of cybersecurity, innovation is not just welcome, it's essential. As business transformation accelerates across every industry, cybersecurity startups are on the frontlines, crafting solutions to protect everything from critical infrastructure to personal data. Venture capital (VC) and private equity (PE) are playing an increasingly vital role in fueling this innovation, injecting the capital and confidence that early-stage and scaling companies need to thrive.

With passionate founders, sophisticated backers, and a rapidly expanding market, the cybersecurity startup ecosystem is more dynamic than ever. Yet, amid this energy and opportunity, there remains a call for clarity: investment in cybersecurity must go beyond growth metrics, it must ensure that these companies practice what they preach.

A GOLDEN ERA FOR CYBERSECURITY STARTUPS

The cybersecurity space has become a magnet for forward-thinking investors, and for good reason. In 2024 alone, global venture investment in cybersecurity startups surpassed $20 billion. With the attack surface of modern enterprises expanding due to AI, and other business transformations, the demand for innovative security solutions continues to soar.

VCs and PEs have seized the moment. The convergence of necessity and innovation has opened the door for high-impact solutions to be funded, nurtured, and scaled globally.

Visionaries like Michael Coates, Founding Partner at Seven Hill Ventures and former CISO of Twitter, are championing the importance of technical depth and operational discipline in early-stage security startups. Similarly, Jay Leek, Managing Partner and Founder of SYN Ventures, is leading a new era of cyber-focused investing, helping build resilient, market-disrupting firms that offer real defense capabilities.

These leaders are setting a high bar, not just for performance, but for internal rigor and ecosystem responsibility.

HOW CAPITAL IS POWERING PROGRESS

1. CATALYZING INNOVATION

Startups thrive on speed. VC funding enables companies to move fast, testing hypotheses, iterating features, hiring elite engineers, and engaging early customers. Many of today's leading cybersecurity firms owe their rapid ascent to early venture investment that gave them the breathing room to build bold and scalable solutions.

This momentum translates into real-world impact: faster threat detection, smarter automation, and broader access to defense tools for mid-market companies and enterprises alike.

2. BUILDING COMPREHENSIVE SECURITY PLATFORMS

While VCs often spark early innovation, private equity excels at helping mature firms scale and integrate. PE-backed rollups and strategic acquisitions are helping create unified security platforms that span endpoint, identity, and cloud security. These rollups, when done thoughtfully, reduce fragmentation and make it easier for CISOs to manage complex environments.

3. PROFESSIONALIZING THE ECOSYSTEM

Investors are also helping elevate operational maturity, supporting startups in building strong governance, compliance frameworks, and go-to-market strategies. This ecosystem support is essential in a space where technical brilliance must be balanced with reliability and trustworthiness.

STARTUPS NEED TO PRACTICE WHAT THEY PREACH

Despite the excitement, cybersecurity startups face a unique paradox: while they sell protection, they must also embody it. As they grow, there's a risk that speed and scale come at the cost of their own internal security posture.

WHY THIS MATTERS

If a cybersecurity vendor is breached, the impact reverberates far beyond brand damage, it threatens client ecosystems, undermines investor confidence, and can result in regulatory penalties. For this reason, investing in cybersecurity isn't just a play on growth, it's a bet on trust.

RISKS WORTH MANAGING

1. INTERNAL HYGIENE MAY LAG BEHIND

Startups scaling rapidly often postpone hardening their own infrastructure. It's not uncommon for vendors to lack multi-factor authentication internally, or to misconfigure access policies, exposing the same risks they're designed to eliminate.

2. SURFACE-LEVEL DUE DILIGENCE

Traditional VC diligence often focuses on growth indicators: ARR, customer logos, and product velocity. But in cybersecurity, diligence must go deeper:

- How secure is the startup's codebase?
- Are DevSecOps principles being applied?
- Has the company undergone recent penetration testing?

3. BREACH FALLOUT CAN BE DISPROPORTIONATE

A breach of a cybersecurity startup has far more reputational consequences than a breach of, say, a logistics firm. The optics are stark—if a cybersecurity company can't defend itself, can it defend others?

SECURING THE INVESTMENT, NOT JUST THE COMPANY

Fortunately, a new wave of cyber-focused investors is flipping the script, making security diligence a core part of their thesis. Leaders like Jay Leek and Michael Coates are advocating for deeper involvement in technical assessments, post-investment governance, and even founder coaching on security-first thinking.

Here's what responsible, progressive investing in cybersecurity startups looks like:

1. INVEST IN SECURITY-BY-DESIGN STARTUPS

Companies that embed secure architecture from the outset—using principles like zero trust, encrypted communications, and identity-based access—are better positioned to scale without compromising trust.

2. CONDUCT TECHNICAL DUE DILIGENCE

Investors should insist on:

- External penetration testing results.
- Code security reviews and static analysis reports.
- Analysis of infrastructure-as-code deployments for vulnerabilities.

This helps identify red flags before term sheets are signed.

3. ENCOURAGE GOVERNANCE, NOT MICROMANAGEMENT

PE and VC firms should take active roles in governance—supporting CISOs, ensuring security KPIs are tracked, and encouraging tabletop exercises for breach readiness. Governance should empower, not constrain, founders.

4. FOSTER A SECURITY CULTURE FROM DAY ONE

Startups should be encouraged to:

- Appoint a CISO or virtual CISO early.
- Adopt DevSecOps methodologies.
- Train non-technical staff on cyber hygiene

Culture is as critical as code when it comes to long-term resilience.

CONCLUSION: OPTIMISM WITH OVERSIGHT

The cybersecurity startup space is one of the most exhilarating frontiers in technology today. It's brimming with talent, urgency, and potential. With capital flowing from savvy investors and thought leaders like Michael Coates and Jay Leek, the ecosystem is poised for unprecedented growth.

But this growth must be accompanied by deliberate diligence. When investors demand not just great products but secure companies, they help elevate the entire industry. They ensure that innovation doesn't just look good on paper, but holds strong under pressure.

Cybersecurity is a trust business. By investing with care, we can build companies that don't just defend networks, but defend the integrity of the ecosystem itself.

K logix

1319 Beacon Street
Suite 1
Brookline, MA 02446

617.860.6485
KLOGIXSECURITY.COM