FEATS OF STRENGTH

A BUSINESS-FOCUSED CYBERSECURITY MAGAZINE

WOMEN IN CYBERSECURITY

September 2025

K logix

TABLE OF CONTENTS

FEATURES

September 2025

MAGAZINE CONTRIBUTORS

Katie Haug - Editor in Chief
VP Marketing, K logix

Kevin West - Editor
CEO, K logix

Emily Graumann - Graphics
Marketing & Design Specialist , K logix

ABOUT K LOGIX

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

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

DEAR READERS,

In this issue of *Feats of Strength*, we celebrate the incredible women shaping the future of cybersecurity. We chose the theme of Women in Cyber because, while representation has grown steadily over the past decade, the industry still faces persistent gaps, particularly in leadership roles. Today, women make up roughly a quarter of the global cybersecurity workforce, but only a small fraction of CISOs and other executive leaders. The stories featured here highlight not only the progress made but also the work still ahead.

Our feature article, *Breaking Barriers: The Growing Role of Women in Cyber*, explores both data and lived experiences, showing how women bring unique perspectives, strategic empathy, and leadership styles that strengthen teams and organizations. Trends like the rise of AI, growing focus on mentorship, and the push for inclusive workplace cultures all play a role in shaping what comes next.

Alongside the article, you'll find profiles of remarkable women leaders, from Colleen Carroll's focus on security at Emburse, to Rachel Manca's work in cyber defense at Boston Scientific, to Tara Fardellone's leadership in GRC at Lionbridge, and more. Each of these leaders embody resilience, expertise, and vision. Together, their stories remind us that the future of cybersecurity depends on broadening the table, empowering diverse voices, and leading with strength.

We hope this issue inspires you to reflect on how we can all help drive greater equity and opportunity in this field. Progress has been made, but the feats of strength still to come will be built by the women, and men, who commit to creating a more inclusive future in cybersecurity.

- Katie Haug, Editor in Chief

PROFILES IN *Confidence*

COLLEEN CARROLL

SENIOR DIRECTOR, SECURITY
Emburse

Headquarters: Dallas, TX

Employees: Private Company

Annual Revenue: Private Company

Colleen Carroll has built her career at the crossroads of technology, risk, and people. With a foundation in technology risk from her early years at Ernst & Young and a master's in accounting, she quickly gravitated toward the governance, compliance, and security space. Over time she has expanded her responsibilities to include compliance, risk management, privacy, application security, and fraud operations. What defines her approach isn't just technical depth, but a clear leadership philosophy: security is a people business.

"In the security world, you do nothing in a silo. You need every team around you," she says, underscoring her belief that collaboration, trust, and communication are the real levers of progress.

SCALING SECURITY IN A HIGH-GROWTH ENVIRONMENT

After six years at EY, Colleen transitioned to Emburse, where she took on the challenge of building a cohesive compliance program in a rapidly expanding, private-equity-backed organization.

"Before we streamlined our approach, audits were handled in silos, with multiple processes that weren't fully coordinated. My focus has been on building a unified structure that reduces redundancy and increases efficiency."

Her responsibilities quickly expanded. "Outside of our 20-plus audits that my team manages, we are SOC 1, SOC 2, ISO, and PCI compliant. I also oversee our GRC activities, all our security risk management and vendor management. And I serve as our data protection officer, so I run our privacy compliance and legal and regulatory adherence as well."

More recently, she has added application security, employee awareness, and fraud risk activities to her portfolio.

EMBRACING AI WITH GUARDRAILS

As Emburse accelerates its use of AI, Colleen has become a key stakeholder in ensuring innovation is balanced with trust.

Across the company, Product and Engineering teams are embedding AI into spend management workflows—from intelligent expense categorization and fraud detection using behavioral signals, to natural language interfaces for reporting and approvals. These capabilities save customers time, reduce errors, and improve compliance, while also laying the foundation for enterprise-scale AI adoption.

Internally, AI is powering enterprise operations such as forecasting, anomaly detection in finance and security, and productivity use cases like code generation, customer support response drafting, and contract review. Together, these initiatives drive efficiency and scalability as Emburse grows.

To guide this innovation responsibly, the company launched AI-Vengers, a cross-functional AI governance and enablement initiative. The program establishes guardrails for responsible AI use—including privacy, bias mitigation, and data security—while promoting safe experimentation across Product, Engineering, Sales, and Support.

Colleen is a central voice in this work. "We've definitely embraced AI and we want to use AI, but obviously within the guardrails of ensuring that our information remains safe," she says. "We've been intentional about providing enterprise-grade AI tools so employees have secure, approved options—balancing innovation with the highest standards for data protection."

THE ONGOING CHALLENGE OF IDENTITY AND PLATFORMS

Like many security leaders, Colleen sees identity as an evergreen challenge. “Identity will always be number one. As soon as you feel like you get a handle on it, there is always more to consider.” People are central to security, which is why building awareness and collaboration across teams is so critical.

She is also pragmatic about the shifting vendor landscape. “We continuously evaluate our vendor landscape to ensure we’re partnering with providers that deliver the broadest, most strategic value—helping us stay both agile and efficient.”

WOMEN IN LEADERSHIP: BUILDING TRUST AND PRESENCE

When asked about navigating a male-dominated industry, Colleen is clear-eyed but optimistic.

“It definitely is male dominated, but I’ve never felt like I wasn’t respected. If you know your stuff and you can talk with confidence, that helps break down barriers.”

She credits the presence of strong female leadership at the top of her organization. “I feel fortunate to be in an organization where we have a very strong leader with a woman as our CEO. And she sets a really great tone from the top down.”

For Colleen, the key to influence is not posturing but relationships. “It’s a people business. If you build relationships and build trust with people, that’s how you start to have your voice respected and heard within those rooms. It doesn’t happen overnight; it’s really building those foundations with the people that you’re working with.”

COLLABORATION AS A LEADERSHIP STYLE

Colleen’s leadership philosophy is rooted in collaboration and adaptability. “No one person has all the answers, which is why collaboration and diverse perspectives are essential to success. You can learn so much from people that you’re working around,” she says. “In the security world, you cannot operate in a silo. You need every team around you.”

She also emphasizes the importance of flexing her leadership style to fit the needs of her team. “Everyone needs a little bit of something different from their manager, so for me it’s asking questions to understand what their working styles are and being able to flex with that.”

PRIVACY AND SECURITY: A CONVERGING FRONTIER

One of Colleen’s current focuses is the convergence of privacy and security. “I am responsible for both of them here. The convergence of privacy and security is evolving rapidly, and our teams are proactively adapting to ensure we meet global requirements and exceed customer expectations. It is essential to establish a privacy program that can adapt and map to the various privacy regulations and changing requirements.”

A CONTINUOUS LEARNER

Colleen is committed to growth, both for herself and her team. “There’s never going to be a point where you feel like you know everything because it’s constantly changing. I am always staying engaged with professional networks.”

Her approach is consistent: build networks, seek out mentors, and learn from adjacent disciplines. As she notes, “Nothing that you do is all that unique. And it’s interesting to hear how other people are working through your same problems and what they’ve found successful.”

LEADING SECURITY IN THE AGE OF AI

Colleen’s career reflects a powerful blend of risk expertise, collaborative leadership, and pragmatic vision. From transforming siloed compliance programs to driving AI governance and embracing privacy as a core pillar, she consistently demonstrates that effective security leadership is about much more than controls—it is about trust, adaptability, and relationships.

At Emburse, her leadership helps ensure that as AI transforms both products and internal operations, it does so responsibly, with the right balance of speed, safety, and trust.

PROFILES IN *Confidence*

CORINA FOURNIER

SENIOR DIRECTOR, SECURITY AND COMPLIANCE

Validity

Headquarters: Boston, MA

Employees: 300

Annual Revenue: Private Company

Corina's career in cybersecurity began long before the industry was a formal discipline. Growing up in Europe, she attended a science and IT focused high school where she built computers, designed websites, and watched friends drift toward the black-hat world. Determined to be on the right side of the law, she set her sights on preventing cybercrime. Moving to the United States at 18, she initially studied biochemistry before ultimately following her passion for technology and earning her degree in IT with a focus on security certifications.

Her early career followed the traditional IT path, from help desk to network and systems engineering, but the pivot to security happened quickly. While working at a financial institution, she was tasked with reviewing 10,000 pages of SIEM logs, a process she instantly knew needed to be automated. From there she dove deeper into security operations, disaster recovery, encryption, and compliance, building an impressive foundation in financial services at a time when few organizations prioritized cybersecurity at scale.

BUILDING PROGRAMS ACROSS INDUSTRIES

After a decade in financial services, Corina moved into healthcare, where protecting sensitive patient data introduced a new set of challenges. There, she gained valuable experience implementing compliance frameworks such as ISO 27001 and SOC 2, while also launching a security program for a software product that credentialed medical staff. This work sparked her interest in software companies and the cloud. She went on to build security programs from the ground up at multiple organizations, helping them achieve critical certifications, migrate securely to the cloud, and establish mature vulnerability management and risk frameworks.

Today, at Validity, Corina serves as Senior Director of Security and Compliance. Her responsibilities span customer trust, privacy and security compliance, vendor risk management, vulnerability management, and incident response. She leads a global team, including an in-house 24/7 SOC, and ensures alignment with frameworks. Her work balances the technical side of security with the governance and risk management needed to scale Validity's operations amid growth and acquisitions.

FOCUS AND CHALLENGES

Looking ahead, Corina is concentrating on three priorities: enhancing incident response preparedness, strengthening cloud security and vendor risk management, and maturing vulnerability management. With cloud misconfigurations continuing to be a root cause of breaches across industries, she is laser-focused on ensuring Validity has both preventive and responsive controls in place.

The challenges are familiar: balancing speed of innovation with risk management, managing third-party risks without full visibility, and protecting a fast-moving business with a lean team. She emphasizes, "Security must be seen as a business enabler, not a blocker, even when decisions need to be made quickly with imperfect information."

LEADERSHIP STYLE

Corina describes herself as a transformational leader. She looks for team members who are "smart, hungry, and humble" and builds her teams around trust and collaboration rather than competition. She believes the right mindset is just as important as technical skills. She empowers her team to innovate, maintains a culture of continuous improvement, and ensures work-life balance without sacrificing high standards. For her, leadership is about creating trusted partnerships across the business while pushing her team to do their best work.

INDUSTRY PERSPECTIVE AND AI GOVERNANCE

With the rapid rise of AI, Corina has taken a proactive role in establishing Validity's AI governance program. She works cross-functionally to ensure AI tools and data should be used responsibly. From vendor due diligence to internal policy, she has built a living framework that adapts as technology evolves. For Corina, the integration of AI represents both a risk and an opportunity, one that demands thoughtful governance to balance innovation with security.

WOMEN IN CYBERSECURITY

Having grown up in a culture where women in science and technology were common, Corina did not initially perceive gender as a barrier. She advanced quickly, landing IT management roles early on in her career. While she has occasionally encountered bias, she reframed those experiences as indicators of cultural misalignment rather than personal limitation. Today, she uses her platform to coach women entering the field, emphasizing grit, curiosity, and the ability to demonstrate initiative, whether through labs, certifications, writing, or community involvement.

Her advice for women early in their careers is straightforward, she says, "Show your grit and excitement. It's not just about experience; companies look for passion and drive. I've seen junior hires with only one year of experience outpace peers with five years, simply because they were hungry to learn and succeed."

LOOKING FORWARD

Corina thrives on the technical side of security as much as compliance and enjoys working with peers across business functions. She stays sharp by engaging in peer groups, conferences, hands-on labs, and ongoing training. For her, the future is about continuously improving programs, strengthening trust with customers, and shaping how security evolves alongside emerging technologies like AI.

She is particularly energized by the challenges AI introduces. "AI is here to stay, and security leaders can't afford to ignore it," she explains. "We need to embrace it responsibly, making sure we put guardrails around how data is used and ensuring our teams understand both the opportunities and the risks." For Corina, this means helping organizations navigate a middle ground: not slowing innovation but ensuring that innovation is done safely and transparently.

Equally important for her is the human side of the equation. "At the end of the day, security isn't just about tools and frameworks, it's about people," she says. "I want to keep creating environments where security teams feel empowered, where colleagues across departments know they can come to us with questions, and where customers feel they can trust us with their most sensitive data." In her view, the next chapter of security leadership is not just about defending systems, but about building a culture of trust, resilience, and shared responsibility.

LIZ MORTON

FIELD CISO
Axonius

Headquarters: New York, NY

Employees: 750+

Annual Revenue: Private Company

PROFILES IN *Confidence*

Liz's career path into information security was anything but linear. Starting out as an art school graduate during the dot-com boom, she quickly pivoted to technology, driven by curiosity and a knack for problem-solving. Early experiences with firewalls, security engineering, and IT operations sparked her awareness of information security as a discipline, but she candidly admits she hesitated to pursue it fully at first.

That changed during her time at Intercontinental Exchange (ICE), where she spent nearly a decade working across IT and closely with the InfoSec team. When the opportunity arose, she stepped into her first full-time InfoSec leadership role, encouraged by mentors who saw her potential even when she may have questioned it herself. That role cemented her passion for the field, and she describes her ICE years as a "PhD in getting things done" where she solved hard problems, led with urgency, and thrived in a high-pressure environment.

Today, as a Field CISO at Axonius, Liz embraces a role that is both dynamic and unstructured. One day she might be speaking with executives at a Fortune 500 company about vulnerability management; the next she's hosting a community dinner, advising venture capital firms, or sharing insights on stage. What makes her perspective unique is that she brings the mindset of a practitioner and an InfoSec leader, not a salesperson. "I talk about people, processes, and technology because I've lived it," she explains. This allows her to connect authentically with prospects and customers, translating technical value into real-world outcomes.

CAREER RESILIENCE AND PIVOTS

Throughout her nearly three-decade career, Liz has navigated challenges and turning points that shaped her leadership. Taking the leap into her job at Axonius was, as she describes it, one of the first times she made a career move without overthinking, a deliberate shake-up that has brought her both growth and renewal.

Her resilience is not just about endurance but about learning when to step away, when to say yes, and when to finally give herself permission to say no. She is candid about these moments because she believes aspiring leaders need to hear that success isn't always a straight line; it's often built through setbacks, risks, and reinvention.

LEADERSHIP WITH CONFIDENCE AND REALISM

Liz's leadership is rooted in empathy, accountability, and pragmatism. Having spent decades as the only woman in the room, she's built confidence in her voice and insists on owning every space she walks into. She challenges traditional advice like "fake it till you make it," instead encouraging women to play to their strengths and reshape the game if it doesn't work for them. For those starting their careers, her guidance is clear: say yes often early on, learn relentlessly, but don't be afraid to eventually curate your path and say no. "If you don't want to take the notes in the meeting or handle the grunt work, don't. Focus your energy where you can add the most value," she advises.

She also underscores the importance of negotiating salary without apology. "Don't give a range. Say the number and let them figure it out. You need to be paid fairly." This directness is part of her philosophy of ownership, taking responsibility for her career trajectory and modeling that same confidence for her mentees.

COMMUNITY AND MENTORSHIP

Beyond her role at Axonius, Liz is deeply committed to mentorship and community involvement. She has worked with organizations like the City of Refuge, where she

helps guide and empower individuals building their careers in technology and cybersecurity. For her, these opportunities are not just about giving back but about ensuring the next generation feels supported in ways she often did not when she was starting out.

She is particularly passionate about helping women in cyber navigate challenges around visibility, workload, and self-advocacy. Liz often reminds her mentees not to accept all the "office housework" tasks such as note-taking, grunt work, or low-visibility projects, these often fall on women in technical roles. Instead, she encourages them to claim the projects that matter most to their career goals and to advocate for themselves unapologetically.

A THOUGHT LEADER ON INDUSTRY TRENDS

From her vantage point at Axonius, Liz has a wide lens on the evolving cybersecurity landscape. She has been struck by how conversations around data quality have become central to AI adoption. In her view, the rush to adopt artificial intelligence will only succeed if organizations focus on the quality, normalization, and reliability of the data feeding these tools. Without that, AI becomes less of an enabler and more of a risk.

Another shift she has observed is the industry's move from traditional vulnerability management toward what is now being called continuous threat exposure management. Instead of treating security as a set of static checklists, organizations are beginning to adopt a mindset of ongoing evaluation and improvement. This mirrors practices in IT operations and represents a more holistic, iterative way of safeguarding systems.

She also notes the growing urgency around identity and deepfake challenges. With AI now capable of producing convincing synthetic voices and images, Liz sees identity verification becoming one of the defining issues of the next decade. The question is no longer just about authenticating accounts, it is about verifying whether the person on the other end is truly who they claim to be. These emerging threats, she emphasizes, will demand both technological innovation and industry-wide collaboration.

LOOKING AHEAD

For Liz, the beauty of her current role is perspective. After years of solving problems within one organization, she now advises many, gaining insights into different industries, team structures, and approaches to cybersecurity. "It's almost like an in-place sabbatical," she says. "I'm learning as much from customers as they learn from me." That balance of expertise, humility, and curiosity defines her work and her voice as a leader in the cybersecurity industry.

PROFILES IN *Confidence*

RACHEL MANCA

SENIOR CYBERSECURITY ANALYST
Boston Scientific

Headquarters: Marlborough, MA

Employees: 50,000

Annual Revenue: $16.7 Billion

Rachel Manca has built her career on curiosity and a drive to understand how technology shapes our lives. Early on, she became fascinated with data privacy and the question of how personal information moves, gets used, and can be protected. That interest led her to internships at TJX and Boston Scientific, where she gained hands-on exposure to security challenges in large organizations. After completing a two-year IT rotational program at Boston Scientific, she found her calling in cybersecurity.

Now, six years later, Rachel serves as a Senior Cybersecurity Analyst, "My work focuses on cybersecurity defense, encompassing incident response and areas like threat intelligence," she explains. She monitors Boston Scientific's digital footprint, investigates alerts, and consolidates metrics across the security program. One project she is particularly proud of is developing an interactive dashboard of KPIs used by leadership. "It's been really fun to see how that's grown and used across a lot of different presentations and value demonstrations," she says.

FOCUS ON EMERGING THREATS AND INNOVATION

Rachel thrives on staying ahead of evolving threats. "I like keeping track of emerging threats and news. It's interesting to wake up every morning and see what's happening." She notes two areas that stand out as priorities: supply chain security and artificial intelligence. She emphasizes the importance of maintaining clear visibility into which vendors are in use and how they connect to the business, ensuring the team can respond quickly and identify what information may be at risk if a security issue arises.

AI represents both an opportunity and a challenge. "AI has many beneficial purposes and it's being used in many good ways, but there is of course the dark side of it," she cautions. "There are a lot of novel techniques that are emerging from threat actors using AI in malicious ways." One key way to protect against these threats, Rachel believes: "Ensuring our user base understands AI literacy and analyzes? What's coming out of AI to ensure its accuracy before it's taken as full fact."

CHALLENGES AND TEAM CULTURE

The fast pace of cybersecurity brings constant pressure to innovate. Rachel notes that it can be easy for teams to fall into routine processes when responding to alerts, but she stresses the importance of continuously questioning whether current methods are the most effective. For her, the challenge is finding smarter ways to respond, and leveraging new tools to ensure the team keeps pace with the speed of evolving threats.

She credits the ability to do so with a collaborative culture. "We have a great team that is used to working together. I came in as an intern and I've learned so much along the way," Rachel says. With a mix of long-tenured employees and new hires, knowledge sharing remains a core strength.

CULTURE OF IMPACT AND BELONGING

Boston Scientific's mission, "Advancing science for life," is central to Rachel's motivation. One example is the annual Everyone Makes an Impact event. "We bring patients on site who have been treated with our products, and they talk about their stories. You walk away feeling the impact of all the work you're doing," she shares. "That definitely brings us together around our core mission and common goal, why we're all here doing what we're doing: providing the best results for the patient, regardless of our functional role."

She is also active in employee resource groups, including EmpowHer and the Young Professionals Network. "Definitely

a sense of community," she says of the benefits she derives from EmpowHer. "It's a special way to connect with members outside of our team and to learn about their experiences and how they've advanced through different challenges." Through peer mentoring programs, goal setting, and volunteering with local organizations, Rachel sees these groups as vital outlets for connection and accountability.

MENTORSHIP AND COMMUNITY ENGAGEMENT

Rachel has benefited from mentors during her career, and she makes it a point to pay that forward. She often works with interns and early-career professionals to help them find their footing in cybersecurity. "I was given so many opportunities as an intern, and I want to make sure others feel the same support I did," she explains. She emphasizes practical advice, how to build confidence in meetings, how to ask questions, and how to map out a career path in security.

Outside the workplace, she stays active in community events, conferences, and panels. These platforms allow her to share her own journey, highlight the value of diversity in cyber, and learn from peers facing similar challenges. She views community engagement not just as professional development, but as a way to give back and inspire the next generation of security professionals.

VISION FOR THE FUTURE OF CYBERSECURITY

Looking forward, Rachel sees cybersecurity becoming even more embedded in everyday business and personal life. "It's not just IT anymore, it touches every part of the business and every individual," she says. She believes the future will require security professionals to be as strong in communication and relationship-building as they are in technical expertise. "It's about being that trusted advisor, not just the person who blocks things."

She also expects rapid innovation in automation, AI-driven defense, and vendor risk management. "The pace of change is only accelerating. Successful organizations will embrace security as part of their culture, not just as a requirement, but as something that adds real value." For Rachel, the ultimate goal is simple: "To keep learning, keep growing, and keep helping others feel empowered in this field."

LEADERSHIP ASPIRATIONS

Looking ahead, Rachel sees herself moving into leadership roles. "I would definitely love to get into people leadership; currently I'm an individual contributor. I think that would be a great area to move into next," she says. In the meantime, she remains focused on continuous learning: "I never stop learning and figuring out how I can apply different things that I'm learning in the community to the role that I'm in."

Breaking Barriers:
The Growing Role of Women in Cyber

By Katie Haug

PROGRESS AND PERSISTENT GAPS

Over the past decade, women's representation in cybersecurity has improved, though the pace is slower than many hoped. In 2015, when we first published a Women in Security issue of the Feats of Strength magazine, women held roughly 11 percent of cybersecurity roles; by 2025, that share has now grown to about 25 percent. Yet more recent data suggests the figure remains closer to 22 percent globally (ISC[2]). Even as the baseline has shifted upward, much of the growth has stalled in recent years (ASIS).

But representation at the top remains elusive. Despite overall gains, women continue to be significantly underrepresented in leadership roles. Only a small proportion of CISOs and executive security roles are held by women (Cyber Magazine). In many organizations, the security teams still include no women at all, a striking indicator of persistent structural barriers (Enterprise Security Tech). These patterns suggest that the challenge lies not just in hiring, but in retaining, promoting, and supporting women throughout their careers.

EDUCATIONAL FOUNDATION & CAREER OWNERSHIP

Women entering cybersecurity tend to come in with strong academic backgrounds, which serve as critical tools of credibility and preparation. In many cases, their higher education, especially graduate work, provides exposure to formal research methods, risk assessment, policy frameworks, and leadership thinking that extend beyond pure technical skills. That broader perspective helps women translate security concerns into business-level conversations, strengthening their influence and value within organizations.

Furthermore, advanced degrees help accelerate the path to leadership by giving women a foundation to advocate for more strategic roles. In an environment where some still question the legitimacy or expertise of women in cyber, credentials help open doors and support internal recognition. Beyond that, education often brings access to networks, mentors, and research communities, connections that fuel professional growth and expand opportunities for impact.

THE VALUE OF WOMEN IN CYBERSECURITY

Increasing the number of women in cybersecurity is not merely a matter of equity, it delivers strategic advantage. Women bring diverse perspectives that can challenge groupthink and broaden thinking around threat patterns, risk modeling, and resilience planning. Because cyber adversaries constantly innovate, having more varied lenses helps defenders spot anomalous patterns that a homogeneous team might overlook.

In junior and mid-level roles, women often excel in bridging technical and business domains. Their communication skills, empathy, and cross-functional orientation help translate security requirements to non-technical stakeholders, ensuring adoption and alignment. At the leadership level, many women emphasize building inclusive cultures, mentoring, and empowering teams, practices that reduce turnover, drive team performance, and foster long-term resilience. In short, women bring not only technical capability but relational intelligence, strategic empathy, and durable team culture to cybersecurity.

WORKING DYNAMICS

Among women in the cybersecurity field, job satisfaction remains relatively high, though with some concerning trends. In the ISC^2 study, about two-thirds of women in cybersecurity reported being satisfied in their roles, comparable to men, though satisfaction has declined in recent years. Yet women are more vulnerable to the negative impacts of workforce shifts: 32% of women said their teams faced layoffs in the past year, compared to 23% of men (TechRepublic).

Other structural disparities persist. Women report experiencing harassment and discrimination at rates far above average, and the pay gap remains significant, women in cybersecurity commonly earn less than men in equivalent roles (TechRepublic). These pressures intensify when women lack peers or mentors, making the journey more fraught for those breaking into technical or executive ranks.

PATHWAYS AND MOTIVATION

Women often enter cybersecurity via non-traditional routes. Some come from tech-adjacent disciplines, others transition from IT, audit, compliance, or privacy. Unlike men who may enter via deeply technical paths, women more often cite mentorship, exposure through adjacent functions, or problem-solving curiosity as their motivators (ISC^2). Recognizing these multiple pathways is key to recruiting and retaining women in the field.

Professional communities also matter significantly. There are numerous organizations created to bring together women in cybersecurity and provide support, peer networks, scholarships, and visibility for women and underrepresented groups. Such communities help provide not just knowledge but confidence and belonging—crucial for retention in a demanding, often lonely field.

LOOKING AHEAD

While we've come from 10% to 22–25% representation, the road to parity is still long. Leadership roles, particularly CISOs and executives, remain overwhelmingly male. Cultural biases, pay inequity, and professional isolations continue to block many women's progression. Yet the growing presence of female security professionals, stronger community ecosystems, and rising awareness offer real momentum.

To sustain this growth, organizations must invest in mentorship, equitable promotion practices, inclusive cultures, and early exposure to cybersecurity for girls and young women. When security strategies benefit from diverse perspectives, organizations become more resilient and responsive to evolving threats. The future of cybersecurity depends not just on stronger technology, but on more inclusive teams, voices, and leaders.

WORKS CITED

"ISC^2 Report: Women Comprise 22% of the Cybersecurity Workforce." ISC^2 Insights, 2025, www.isc2.org/Insights/2025/03/Women-Comprise-22-percent-of-the-Cybersecurity-Workforce.

"Women's Role in Filling the Workforce Gap." ISC^2 Insights, 2024, www.isc2.org/Insights/2024/04/Women-in-Cybersecurity-Report-Inclusion-Advancement-Pay-Equity.

"Women Lose Jobs at Disproportionate Rate in Cyber Layoffs." TechRepublic, techrepublic.com/article/women-in-cyber-security-2024-isc2.

"Women in Cybersecurity: 2022 Report." Cybersecurity Ventures, 2022, cybersecurityventures.com/wp-content/uploads/2022/09/Women-In-Cybersecurity-2022-Report-Final.pdf.

PROFILES IN *Confidence*

SUNEETHA GOLLA

DIRECTOR OF IDENTITY AND ACCESS MANAGEMENT

Premise Health

Headquarters: Brentwood, TN

Employees: 6,000+

Annual Revenue: $1.5 Billion

Suneetha Golla's journey into cybersecurity began with a leap of curiosity and a willingness to learn. Originally from India, she earned her bachelor's degree in engineering before moving to the United States to pursue a master's in computer science at Western Kentucky University. Her early career started in programming, but while working at LifePoint Health, she was unexpectedly asked to support IT audit efforts. What began as "tag, you're it" quickly grew into a passion for information security, leading her to pursue certifications and hands-on experience in IT security audits across HIPAA, PCI, SOC 2, FISMA, and more.

That blend of technical expertise and audit exposure and strong professional relationships positioned her to join Premise Health, where she has grown over the past nine years to become Director of Identity and Access Management (IAM). She now leads a team of analysts and engineers managing IAM operations, privileged access management, and access certification programs. Her work spans from maintaining IAM solutions and Active Directory to advancing Premise's roadmap toward automation and emerging technologies like passwordless authentication. Along the way, she has become a trusted leader who has built credibility both within her department and across the broader organization.

LEADERSHIP IN ACTION

For Suneetha, leadership has been as much about communication as it has about technology. Transitioning from manager to director required her to shift into a role where she not only manages projects but also communicates upward to senior leadership, aligning IAM initiatives with business goals and securing buy-in. "It's a lot of communication across the board," she explains. "You stay in touch with leaders, give them a glimpse of what's going on in IAM, and seek opportunities to help them as well."

She sees her role as equal parts strategist and advocate. By creating clear roadmaps, aligning her team's priorities with organizational needs, and translating technical risks into business terms, she ensures IAM is viewed not as a cost center but as a critical enabler of security and compliance. This approach has helped elevate IAM from a behind-the-scenes function into a trusted partner across the business.

CURRENT FOCUS AND CHALLENGES

Suneetha and her team are laser-focused on reducing manual processes and implementing automation to make IAM more efficient and proactive. Yet, like many in healthcare cybersecurity, she faces the challenge of ambitious goals with limited resources. "It's the same team keeping up with the technology stack, doing operations, supporting organizational projects, and moving IAM initiatives forward," she notes.

She views these challenges as opportunities to innovate. Her team finds ways to extract more value from existing tools, streamline workflows, and reallocate resources to focus on high-impact projects. This resourcefulness has not only strengthened IAM's reputation within Premise but also positioned the team as resilient and adaptable in the face of constant change.

A "NO DRAMA" LEADERSHIP STYLE

Describing her approach as "no drama," Suneetha prioritizes clarity and collaboration. She believes in solving problems within the right security guardrails but lets her team contribute ideas and shape solutions. She emphasizes relationship-building across departments, which has been critical in establishing IAM's credibility. Feedback, both

giving and receiving, is another cornerstone of her leadership philosophy, helping her stay connected, adaptable, and ever evolving as a leader.

Her style with emphasis on empathy and emotional intelligence resonates because it creates space for trust. By empowering her team to take ownership of projects and decisions, she fosters an environment where people feel safe to learn, experiment, and grow. For Suneetha, leadership is not about micromanagement but about setting people up for success and providing cover when they need it most. This philosophy has contributed to strong team cohesion, loyalty, and talent retention.

CHAMPIONING DIVERSITY AND GROWTH

As a woman in cybersecurity leadership, Suneetha is intentional about opening doors for others. She partners with HR to increase gender diversity on her team, advocates for qualified female candidates, and mentors women in the industry. She also participates, volunteers and serves in local cyber professional groups, strengthening her network and championing women in security leadership.

She is passionate about creating opportunities not just for her own advancement but for the next generation of security professionals. By mentoring students and early-career women, she helps demystify the industry and encourages them to see a future for themselves in cybersecurity. For her, progress in diversity is about more than numbers, it's about fostering environments where women feel empowered to contribute fully, advance confidently, and see leaders who look like them.

INDUSTRY PERSPECTIVES & THE FUTURE OF IAM

Suneetha has a keen eye on where identity and access management is headed. She sees automation, passwordless authentication, and continuous improvement in access governance as the next big steps for the field. These innovations promise not only to reduce risk but also to improve user experience, making security seamless rather than burdensome.

Looking ahead, she believes the future of IAM will be defined by adaptability. The increasing complexity of IT environments, coupled with evolving threats, demands security leaders who can anticipate change and respond quickly. For Suneetha, that means staying curious, staying connected to the industry, and continuing to invest in both her own learning and her team's growth. She sees IAM not as a static function but as a constantly evolving discipline that will play a central role in healthcare security for years to come.

PROFILES IN *Confidence*

SUZIE SMIBERT

CTO
DTG Recycling

Headquarters: Bothell, Washington

Employees: 580+

Annual Revenue: Private Company

BRIDGING TRANSFORMATION AND SECURITY

Suzie Smibert's journey has been defined by transformation and resilience. Her career path has taken her through private equity turnarounds, large-scale financial services modernization, and now into her current role as Chief Technology Officer overseeing cybersecurity, privacy, and enterprise technology at DTG Recycling.

Suzie's leadership philosophy is rooted in her ability to bridge the gap between technology and business priorities. She views her role not just as a technologist, but as an executive who ensures that innovation and cybersecurity directly enable growth. "To be good at cybersecurity, you must understand what the business is trying to accomplish across the organization," she explains. This perspective has guided her across her career where she has consistently aligned complex technology initiatives with business strategy, balancing innovation with risk in a way that drives tangible value.

RESILIENCE AND REDEFINING CAREER PATHS

Suzie is equally recognized for her ability to lead with resourcefulness, especially in environments where budgets are tight and expectations are high. Throughout her career, she has rarely had the luxury of infinite resources. Instead, she became skilled at finding creative solutions. This mindset not only delivered strong results at a fraction of the cost but also fostered innovation and agility within her teams. Her approach demonstrates a key aspect of her leadership: making bold, strategic choices that advance the business, even when operating under constraints.

DRIVING CHANGE THROUGH TECHNOLOGY

"Every company is a technology company," she emphasizes. "And through technology you can change business processes."

Suzie's ability to deliver transformation at scale was further demonstrated at a Canadian banking provider (later acquired by CGI), where she was hired to lead cybersecurity, privacy, and client relations following a damaging cyber incident that had impacted several credit unions. She worked not only to stabilize the organization but also to raise the standard for transparency, disclosure, and partnership with credit union clients: "We were focused on doing the right thing for the members and those that bank with them."

Today, at DTG Recycling, Suzie oversees the full technology portfolio, from cybersecurity and privacy to enterprise IT operations. The scope is vast, but she views it as a natural extension of her career. She explains, "Whether it's an application or end user support, you need to be in tune with how they're architecting, delivering, and providing services."

LEADERSHIP IN ACTION

Suzie's leadership style is grounded in pragmatism, business acumen, and decisiveness. She understands that technology leaders must often make difficult tradeoffs, recognizing that the ultimate goal is not simply stronger security, but stronger business outcomes. For her, that means ensuring security decisions never come at the cost of customer experience, revenue generation, or the organization's ability to deliver on its core mission.

Her view of security is always framed through the lens of enabling business. "You can't put security at the expense of

servicing your customer or impacting the business in such a way that materially affects their ability to make or sell their product," she says. That business-first mentality is what she considers the hallmark of a true executive leader.

She also emphasizes the importance of aligning technology strategy with business goals, describing it as a creative and transformative force. "The power of having a solid technology strategy that is aligned with the business strategy can transform an organization really fast in a very positive way," she notes.

INNOVATION AND AI: BALANCING PROMISE WITH RISK

One of Suzie's current priorities is harnessing the power of artificial intelligence in ways that optimize safety, efficiency, and customer experience. At her current organization, AI-driven video analytics now monitor facilities to improve operational safety by helping in areas like detecting whether protective gear is worn or streamlining customer service.

She explains, "We've been using AI from both a safety and efficiency perspective, like license plate scanning to pre-populate systems so we don't have to ask customers the same questions."

Yet she remains cautious. Her concern lies not only in technical vulnerabilities but in the social impact of unchecked AI models. "The use of AI is transforming how humans interact with technology... What type of bias or loopholes are in these systems and how will they impact how people think or behave? Could it radicalize?" she warns.

This dual lens, embracing innovation while scrutinizing risks, captures the essence of her leadership approach around the ever-expanding AI topic.

WOMEN IN LEADERSHIP: OWNING THE ROOM

As part of the broader theme of women in cybersecurity, Suzie reflects candidly on navigating male-dominated spaces. Her philosophy is unapologetic: "I've got purple hair. I've got an accent. I'm not apologizing. I don't wear high heels anymore. I wear the brightest, loudest runners there are. I'm in people's face, and I've earned that".

With two decades of executive experience, she advises other women leaders to embrace authenticity over conformity: "You don't need to wear a pantsuit with a turtleneck if that's not who you are. People will see through it if you're playing a role. Just play yourself, and trust that you deserve a promotion."

She also shares practical strategies for commanding presence in boardrooms. Rather than sit quietly in a corner, she encourages women to position themselves close to the chair of the meeting and to take up space, spreading out their notes, coffee, or laptop to avoid making themselves small. Language matters as much as body language, she notes, urging women to speak with confidence, avoid diminishing words that sound like they are asking permission, and to state their ideas directly. And when a male colleague repeats something a woman has already said, she suggests reclaiming the moment with a simple acknowledgment: "Thank you for reinforcing what I just said." These techniques, combined with authenticity and earned credibility, allow women to not just occupy a seat at the table, but to truly own the room.

UNAPOLOGETIC AUTHENTICITY

Suzie exemplifies what it means to lead at the crossroads of cybersecurity, business transformation, and executive strategy. Her career demonstrates resilience in the face of bias, vision in the application of technology, and an unwavering commitment to authenticity.

Her story is both a testament to the evolving role of technology leaders and an inspiration for women in cybersecurity: to speak with confidence and transform organizations not just through code and controls, but through vision, courage, and unapologetic authenticity.

TARA FARDELLONE

DIRECTOR OF GOVERNANCE, RISK AND COMPLIANCE

Lionbridge

Headquarters: Waltham, MA

Employees: 6,000

Annual Revenue: Private Company

PROFILES IN *Confidence*

Tara's journey into cybersecurity was anything but traditional. She earned her degree in Earth and Atmospheric Science from Cornell, but her curiosity in technology grew as she taught herself HTML, built websites, and even launched a side business in web development. That hands-on work eventually exposed her to cybersecurity, especially after experiencing her first hack.

Later, while working in marketing operations at Lionbridge, Tara's passion for technology merged with opportunity. She transitioned into the Trust Team under the CISO's mentorship, who encouraged her to lean into her curiosity and willingness to learn, exposing the art of the possible to her. That shift solidified her career in governance, risk, and compliance.

EXPANSIVE RESPONSIBILITIES IN GRC

As Director of Governance, Risk, and Compliance, Tara wears many hats. She oversees policies, training, and awareness campaigns, while also managing audits, internal controls, and third-party risk.

Her role extends beyond compliance. She also oversees application security, penetration testing, and contributes to incident response strategy.

What excites Tara most is the variety of her work. Each day brings new challenges, from customer-facing conversations about data protection to supporting threat hunts with her team. For her, the heart of the role is not just compliance, but building trust and meaningful relationships with customers.

SUPPLY CHAIN RISK: A TOP PRIORITY

Tara sees supply chain risk as one of the biggest challenges in cybersecurity. Lionbridge often operates deep within the supply chains of some of the world's largest companies, making visibility and accountability critical in Lionbridge's supply chain, as well.

She explains, "We can't protect what we can't see." Her focus is on holding third parties to the same high standards that Lionbridge commits to, ensuring resilience across the broader ecosystem.

EMBRACING AI WITH TRANSPARENCY AND INNOVATION

Artificial intelligence has become a defining focus in Tara's current role. She is deeply engaged in shaping how AI is applied within her work, ensuring that it is used responsibly and with a clear sense of accountability. For Tara, this isn't just about embracing new technology, it's about building trust. She has made it a priority to put transparency and compliance at the center of every AI initiative she leads.

One of her earliest steps was introducing a "transparency commitment" designed to document Lionbridge's ethical adoption of AI tools. This included close collaboration with her colleagues who performed formal risk assessments, created careful documentation, and developed practical guidelines that Lionbridge employees could follow. Tara believes these guardrails are essential, not only to protect customers but also to give her team the confidence to experiment and innovate with AI in a safe, thoughtful way.

Beyond policy, Tara has been vocal about reframing how AI is perceived in the workplace. While some view it as a potential disruptor to jobs, she takes a different stance. In her eyes, AI is not a replacement for human talent but a powerful complement. She sees it as a way to remove the repetitive, time-consuming tasks that often get in the way of deeper, more strategic work.

This philosophy has shaped how Tara leads her team. By encouraging the safe use of AI to handle routine functions, teammates are able to focus on the kinds of work that demand creativity, judgment, and critical thinking. For Tara, this balance is key: “It frees us up to do the things we love to do and allows AI to take care of tasks requiring less critical thinking,” she explains.

In every aspect of her approach, Tara positions AI as an enabler rather than a threat. Her perspective reflects both optimism and practicality, acknowledging the challenges that come with new technology while showing how it can elevate the human side of work. By centering her efforts on transparency, accountability, and empowerment, Tara is setting a standard for how AI can be integrated thoughtfully and effectively.

A WOMAN IN CYBERSECURITY

Tara is no stranger to male-dominated industries. In her meteorology program, she was one of only two women in her graduating class. That experience shaped her confidence and independence while teaching her that anything is possible for any person, regardless of gender, limiting beliefs, or lack of experience.

She acknowledges others may face barriers, but her approach has been to let her work and expertise speak for themselves. At Lionbridge, she has found a culture that celebrates diversity and inclusion, repeatedly earning recognition as one of the best places for women to work.

For Tara, gender has never been the defining factor. Success has always been about the quality of the work, the value delivered, and the courage to try.

LEADERSHIP WITH EMPATHY AND OWNERSHIP

Tara’s leadership philosophy blends empathy, accountability, and curiosity. She adapts her style to meet team members where they are, while uniting them under a shared vision. Her approach is grounded in the belief that people do their best work when they feel both supported and challenged.

She adopted a core part of her philosophy from a book written by two Navy SEALs; Jocko Willinik and Leif Babin called, “Extreme Ownership.” When things go well, she is quick to highlight her team’s contributions and celebrate their success. But when challenges arise, Tara takes personal responsibility. “If something doesn’t go as planned, that’s on me,” she explains. “It’s my job to learn from it and clear the path so my team can move forward.” This mindset has created a culture of trust, where people know they are safe to take risks and innovate.

Equally important to Tara is curiosity. She doesn’t expect her team to arrive with all the answers, but she does expect them to stay open, adaptable, and eager to learn. She reinforces this by asking thoughtful questions, encouraging debate, and showing genuine interest in new ideas. “Curiosity is how we grow,” Tara says. “It’s not about being perfect, it’s about being willing to ask, to try, and to stretch.”

Her leadership is also hands-on. Tara never asks her team to do work she hasn’t done herself, and she isn’t afraid to dive into details alongside them. This creates a sense of partnership rather than hierarchy. Her team knows she is not only their leader but also their collaborator, invested in both the work and their personal growth.

For Tara, leadership is ultimately about creating a safe and motivating environment full of opportunity. She strives to make sure every person feels valued and supported, while still being pushed to achieve their best. By combining empathy with accountability and curiosity, she has built a leadership style that inspires loyalty, confidence, and continuous improvement.

K logix

1319 Beacon Street
Suite 1
Brookline, MA 02446

617.860.6485
KLOGIXSECURITY.COM

WOMEN IN CYBERSECURITY

NEW ENGLAND WOMEN IN CYBERSECURITY:

Join the **Boston Women in Cyber Event** on October 23rd in Back Bay!

Hear from trailblazing female leaders, enjoy networking and pop-up activities.

Register:
https://www.klogixsecurity.com/-women-in-cyber-event-1