

Influential Women Features Aparna Kadari, CISM, CISA: Director of Cybersecurity at Delviom, LLC

VA, UNITED STATES, August 25, 2026 /EINPresswire.com/ -- Cybersecurity Leadership Is No Longer Just About Security – It Is About Running the Business Better

Ashburn, Virginia — Aparna Kadari's unconventional path from data entry to cybersecurity leadership offers a lesson for an industry being reshaped by AI, automation, cloud transformation and an escalating battle for cyber talent.

Cybersecurity has spent years trying to earn a seat at the business table. The next generation of security leaders may have a different challenge: proving that they understand the entire business sitting around it.



For Aparna Kadari, CISM, CISA, Director of Cybersecurity at Delviom, LLC, that perspective did not come from following a traditional cybersecurity career path. It came from doing almost everything else first.

Aparna began her career in data entry before moving through IT project management, technical leadership, production support, enterprise operations and large-scale program management. Eventually, that path led to cybersecurity leadership.

It was hardly a straight line. That may have been its greatest advantage.

Today, Aparna leads cybersecurity strategy, engineering, operations and risk initiatives across complex federal and commercial environments. But she still describes herself first as an operator – someone who looks at cybersecurity not simply through the lens of controls and

threats, but through the interconnected realities of technology, people, budgets, mission and business performance.

That distinction matters as cybersecurity enters a new era.

Security Is Becoming an Operating Model – The modern security leader is no longer responsible only for defending networks or demonstrating compliance. Cloud transformation, Zero Trust, artificial intelligence, automation and increasingly interconnected technology ecosystems have pushed cybersecurity much closer to the center of enterprise decision-making.

The question is no longer simply, Are we secure? It is also: Can we operate securely at scale? Can leaders understand risk quickly enough to act? Can security keep pace with the business rather than become the reason it slows down?

Aparna's approach is built around that intersection. Her work has included modernization roadmaps, vulnerability remediation, patch management, security engineering, workforce development and broader cybersecurity transformation. Across those efforts, the objective remains consistent: turn security strategy into something measurable, operational and sustainable.

That philosophy also reflects lessons learned outside cybersecurity.

Having managed enterprise budgets exceeding \$110 million while maintaining variances below 0.1%, Aparna learned early that strategy ultimately has to survive contact with execution. Ambitious programs mean little if organizations cannot fund them responsibly, operationalize them effectively or demonstrate outcomes. Cybersecurity is no exception.

The Human Cost of "Always On"

There is another issue Aparna believes cybersecurity organizations cannot afford to overlook: the people operating the systems. The industry has normalized an "always on" culture – rotations, escalations, incidents and constant urgency. But resilience cannot be measured only by system uptime.

It also has to include workforce sustainability.

Throughout her leadership career, Aparna has focused on improving operational stability while reducing unnecessary fatigue created by continuous rotational demands. The goal is not to lower expectations. It is to design better systems, processes and automation so highly skilled professionals spend less time fighting preventable fires and more time solving consequential problems. That becomes increasingly important as organizations struggle to recruit and retain cybersecurity talent.

Technology can automate a workflow. It cannot automatically create a healthy operating

culture.

AI Will Change Cybersecurity. Adaptability Will Decide Who Leads It.

Artificial intelligence is accelerating both sides of the cybersecurity equation. Attackers are gaining tools that can increase speed and sophistication. Defenders are gaining capabilities that can correlate risk, automate analysis and identify patterns at a scale humans alone cannot reasonably manage.

Quantum computing introduces another layer of long-term disruption.

Aparna sees those developments less as reasons for fear than as reminders that cybersecurity careers cannot remain static.

The leaders who succeed over the next decade may not necessarily be those who know the most today. They may be those most willing to continuously learn what they do not know tomorrow.

Her advice is simple: Fail Forward.

For professionals entering cybersecurity, that means resisting the belief that they must already understand everything before they belong in the field. Certifications matter. Technical foundations matter. But hands-on experience, curiosity and the willingness to tackle unfamiliar problems can be equally transformative.

Cybersecurity itself provides room for remarkably different careers, from engineering, cloud security and operations to governance, risk, artificial intelligence and threat intelligence.

There is no single doorway into the profession. Aparna's own career may be evidence of that.

Why Cybersecurity Still Needs More Women

The global cybersecurity workforce gap also creates an extraordinary opportunity, particularly for women who may not initially see themselves as traditional cybersecurity candidates.

Aparna's message to them is not simply to enter the profession. It is to recognize the value they bring once they arrive. Learn continuously. Build technical credibility. Advocate for yourself. Pursue opportunities before you feel completely ready. And do not define success according to someone else's career timeline.

Aparna has carried that philosophy into her mentorship and advocacy work, including involvement with Women in Technology and broader cybersecurity communities. For her, mentorship is not an extracurricular leadership activity. It is part of building the industry's future workforce.

That belief is rooted in her own experience.

Aparna credits her mother as her first mentor and her husband, Ram Shivareddy, as a longtime technical mentor. She also points to leaders and colleagues including Stephen Brannon, Jeffrey Kadans, Vasanth Barre, Kevin McDonald, Deedie Weaver, Supriya Ahuja, Teresa Alvarez and Michael Magill whose guidance helped shape different stages of her career.

The lesson she carried forward was that careers are rarely built alone.

The Advantage of Being Different

Perhaps the most enduring advice Aparna received was also among the simplest: if you want to be noticed, bring something unique and have the courage not to look like everyone else.

In technology, where credentials and career paths can begin to look remarkably similar, differentiation increasingly comes from perspective. For Aparna, that perspective was built through an unconventional journey across operations, technology, program management, finance and cybersecurity. It taught her to see security problems not as isolated technical events, but as enterprise problems with technical, operational, financial and human consequences.

That may increasingly be what organizations need from their security leaders.

Cybersecurity's future will certainly involve better tools, more automation, AI-driven analysis and increasingly sophisticated defenses. But tools alone will not create resilient organizations. People will.

And the leaders who stand out may be those who can connect the two: understanding the technology deeply enough to protect the enterprise, the business well enough to enable it, and the people well enough to make both sustainable.

Aparna's career offers a useful reminder for an industry obsessed with predicting what comes next:

The future of cybersecurity may belong not to the people who followed the perfect path, but to those who learned enough from every imperfect turn to see the whole system differently.

Learn More about Aparna Kadari:

Through her Influential Women profile, <https://influentialwomen.com/connect/aparna-kadari>

Influential Women

Influential Women provides a platform where women from all backgrounds can connect, share their perspectives, and create content that empowers themselves and others. Through storytelling, thought leadership, and creative expression, Influential Women amplifies voices that

inspire change.

Editorial Team

Influential Women

[email us here](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/936883726>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2026 Newsmatics Inc. All Right Reserved.