PROFILES IN *Confidence*

# MICHAEL NEWBORN

## CISO
## Navy Federal Credit Union

**Headquarters:** Vienna, VI

**Employees:** 25,100

**Annual Revenue:** $12.5 Billion

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."