PROFILES IN *Confidence*

EVAN WHEELER

Senior Director Technology Risk Management

Capital One

Headquarters: McLean, Virginia

Employees: 76,300

Annual Revenue: $15.6 Billion

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

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

FROM CYBERSECURITY TO RISK LEADERSHIP

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

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

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

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

EXPANDING RISK BEYOND THE ENTERPRISE

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

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

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

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

THERE IS NO SINGLE CISO PLAYBOOK

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

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

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

INVESTING IN HIGH-LEVERAGE CONTROLS

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

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

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

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

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

AI WILL ACCELERATE EVERYTHING

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

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

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

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

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

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

AI AS A BUSINESS IMPERATIVE

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

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

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

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

BALANCING AUTOMATION AND TALENT DEVELOPMENT

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

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

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

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

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

THE FUNDAMENTALS STILL MATTER

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

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

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

LOOKING AHEAD

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

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

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

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