PROFILES IN *Confidence*

DAN BOWDEN

GLOBAL BUSINESS CISO
Marsh McLennan (MMC)

Headquarters: New York, NY

Employees: 90,000+

Annual Revenue: $24.5 Billion

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.