PROFILES IN *Confidence*

RICH MARCUS

CISO
AuditBoard

Headquarters: Cerritos, CA

Employees: 800+

Total Number of Customers: 2,300+
More than 50 percent of the Fortune 500, and 7 of the Fortune 10, use AuditBoard's modern connected risk platform

LEADING FROM THE MIDDLE: RICH MARCUS' VISION FOR CYBERSECURITY AT AUDITBOARD

For Rich Marcus, cybersecurity is as much about mindset as it is about tools. As CISO of AuditBoard, he sees his role not only as a technical leader but also as a bridge between business, operations, and risk.

"I've always liked working in the middle of things," Rich says. "I like building connections across an organization. That's really where the CISO role lives, at the intersection of business and security."

That position, he says, requires empathy and communication. "You must understand what different teams care about. Legal might be thinking about contracts, engineering might be thinking about velocity. My job is to align security with those priorities without slowing them down."

SECURITY AT A GROWING SAAS COMPANY

AuditBoard is a SaaS-based risk management platform trusted by some of the most security- and compliance-conscious organizations. "We're a company that sells to audit, risk, and compliance professionals. So, we don't get a lot of leeway if we're not doing security well," Rich says.

Operating at that level means security must be built in, not bolted on. "When you're a SaaS company, your software is your product. If the product isn't secure, your entire business is at risk. Our customers expect that we meet the bar and increasingly, that we help raise it."

That also means that demonstrating compliance isn't enough. "Customers want to see evidence. They want to know how you manage data, how you control access, what happens in an incident. It's not just check-the-box anymore. It's operational."

ENABLING GROWTH WITHOUT SLOWING IT DOWN

Security programs at scale often struggle with speed, but Rich is committed to enabling, not obstructing, growth. "I don't want to be the reason a product launch is delayed. Security can't be an afterthought, but it also can't be a roadblock."

That means deep partnerships with product and engineering. "We work alongside those teams, not above them. When we're in planning meetings, roadmap discussions, sprint reviews, we're contributing value, not just saying 'no.'"

He also emphasizes automation and tooling as enablers. "Manual processes don't scale. If you can't automate access reviews, patch management, or alerting, you'll get buried. So, we invest in systems that reduce friction."

RETHINKING THE RISK CONVERSATION

For Rich, real cybersecurity maturity means separating hype from substance. "There's a lot of noise in this space. But if you look at the root cause of most breaches, it's the basics: exposed credentials, unpatched systems, excessive privileges."

He focuses his team on strengthening these fundamentals. "We're ruthless about identity management. We segment access. We monitor privilege escalation. These aren't glamorous, but they work."

He also critiques the overuse of fear-based messaging. "I don't need to scare people into caring about security. I need to make it relevant to their job. If someone in marketing understands how phishing impacts brand trust, they'll be

more invested."

AI: AN OPPORTUNITY WITH GUARDRAILS

AI presents both promise and risk. Rich approaches it pragmatically. "Everyone wants to leverage AI, and we do too, but we have to be deliberate. We have policies in place for generative AI use, and we've defined what data can and can't be used."

Internal governance is key. "We don't ban tools just to ban them. We evaluate risk, define acceptable use, and educate users. That builds trust and ultimately leads to safer adoption."

He's also watching the AI space evolve. "AI will change how security teams operate, from detection to response. But it won't replace fundamentals. We still need smart people making good decisions."

A BOARD THAT GETS IT

At AuditBoard, Marcus has something many CISOs envy: engaged, informed leadership. "Our board understands that security is existential. They ask smart questions. They're not just looking for dashboards, they want context."

That relationship is built on transparency. "We don't sugarcoat things. If there's a risk, we say so. And if we don't have something fully solved yet, we say that too. That openness builds credibility."

He regularly shares not just performance metrics, but lessons learned. "If we had a near miss or a false positive, we talk about it. That shows we're not just measuring success, we are demonstrating resilience."

THE CISO'S REAL JOB: INFLUENCE

Technical skills are critical, but for Rich, influence is what defines an effective CISO. "If I can't convince people why something matters, it doesn't get done. Influence is the lever."

He's deliberate about tailoring his message. "When I talk to engineers, I get technical. When I talk to executives, I talk about business impact. You must speak the language of your audience."

That adaptability helps drive alignment. "We want security to be a shared responsibility. That means making it part of how the company operates, not just something the security team owns."

RESILIENCE OVER PERFECTION

Ultimately, Marcus doesn't aim for zero risk, he aims for resilience. "We're not naïve. We know we can't stop every threat. But we can design systems that recover fast, that limit blast radius, that learn and improve."

That mindset informs everything from architecture to incident response. "We train for failure. We practice scenarios. We ask: what if this breaks? How do we contain it? How do we learn from it?"

For Rich, it's this operational rigor, not flashy tools or marketing buzzwords, that will define the next generation of great security programs. "Resilience isn't reactive. It's built in. And that's what we're focused on every day."