PROFILES IN *Confidence*

RICK ORLOFF

CISO
Pure Storage

Headquarters: Santa Clara, CA

Employees: 6,000

Annual Revenue: $1.5 Billion

UNDERSTANDING THE RISK LANDSCAPE

Rick Orloff is currently the CISO at Pure Storage, and brings over 20 years of experience as a technical and business enabler, bridging gaps and bolstering security programs. When Rick steps into a boardroom, he brings more than expertise, he brings a reality check. A veteran of cybersecurity leadership roles at Apple and other organizations throughout Silicon Valley, Rick has built a career around confronting misconceptions about digital risk. “Most people believe that we have controls in place and they’re strong enough, and the truth is, they’re not,” he warns.

According to Rick, many executives view cyber threats through an outdated lens. “We’re dealing with a different threat model today.” The core issue? “Somebody got access to something they shouldn’t have. So what is the root problem?.” He emphasizes that the focus must shift from headline-making breaches to the basic principles of access control. “The vast majority of successful attacks are identity based.”

THE IDENTITY AND ACCESS CRISIS

For Rick, a lot begins and ends with identity. “You must govern access and identities,” he says. “And if you don’t have a governance program, you’re likely going to be breached or already have been.”

Identity is no longer a background function, it’s the foundation. “If you know how to govern identity and access, you’re probably halfway there in terms of protecting your organization.” He frequently sees companies investing heavily in security tools without understanding how poorly governed identities are leaving the door wide open. “Even if you have an identity program, if it’s not governed and if it’s not properly supervised and audited, then it’s probably a vulnerability.”

The challenge, he adds, is scale. “You have to know what vendors you have, what access they have, and who manages them. Most companies can’t answer those questions.”

CYBERSECURITY IN THE BOARDROOM

Rick believes boards of directors must play an active role in cybersecurity oversight, but that doesn’t mean they need to become technologists. Instead, he encourages them to ask focused questions.

He urges board members to go deeper. “Ask the same question in three or four different ways. If you get a different answer, you have a problem.” Clarity and consistency are key. “You want to create a culture where cybersecurity is not separate from the business, it is engrained with the business.”

He also emphasizes the importance of aligning cyber risk with business risk. “Every business function has cyber implications, and every board decision has cyber consequences. So, it’s not just an IT problem, it’s a business resilience conversation.”

RETHINKING SECURITY INVESTMENTS

Despite the flood of new security tools hitting the market, Rick cautions against blind spending. “I think the most overvalued security program area is SIEM,” he says. “People have over-rotated and over-invested without properly thinking about what outcome they want.”

Instead, he advises a more disciplined, business-first approach: “What are the crown jewels? How do we protect those? How do we understand how they’re being used and accessed?”

His message: don’t buy the tool until you understand the problem. “People buy all this tech, but don’t know how to operationalize it. It’s shelfware.”

AVOIDING THE COMPLIANCE TRAP

Rick has seen too many security programs driven more by audit requirements than actual risk. “Is the program driven by compliance, or is it driven by risk?” he challenges. “Because those are two very different things.”

Compliance may check boxes, but it doesn’t prevent breaches. “You can be 100% compliant and still 0% secure,” he says. “The objective should be business continuity and risk mitigation, not passing an audit.”

He emphasizes that success comes from prioritizing outcome-based thinking: “What business function are we enabling or protecting with this investment?”

SIMPLIFYING SECURITY FOR THE BUSINESS

One of Rick’s core goals is to demystify cybersecurity for non-technical leaders. “Cyber is not about complexity,” he says. “It’s about understanding your data, understanding your identities, and controlling access.”

He believes the best CISOs are those who speak the language of business. “I want the board to understand why we’re doing what we’re doing and what the outcomes should be. If they can’t repeat what you just said back to you, you’re not communicating effectively.”

Rick also coaches CISOs to align their programs with corporate strategy. “If you can show how your cyber investments support growth, innovation, and resilience, then you’re not just a security leader, you’re a business leader.”

FROM PRACTITIONER TO ADVISOR

Rick’s influence today goes beyond operational leadership, he’s a trusted advisor to boards, executives, and emerging cybersecurity leaders. He sees himself as both an educator and a challenger. “Occasionally my job is to make people uncomfortable in a constructive way,” he says. “Because discomfort leads to awareness, and awareness leads to change.”

For organizations looking to future-proof their cybersecurity posture, Rick’s advice is clear and grounded in experience: govern access, ask the right questions, and stay focused on business outcomes.

“If you can’t tell me who has access to what, why they have it, and how it’s being used, then you’re not secure. And no amount of technology will fix that.”