KONRAD **FELLMANN**

CISO
Encore Capital Group

Headquarters: San Diego, CA

Employees: 7,300+

Annual Revenue: $1.5 Billion

A CAREER BUILT ON IMPACT

Konrad Fellmann's career journey began as a Marine Corps officer, working in logistics. He then became an implementation consultant for a product data management software company, coding, and customizing software. However, he soon realized he was interested in different types of responsibilities. "I just got bored, it was too easy, and I needed another challenge." That led to a long consulting career across industries and eventually building a global security program at Cubic before joining Encore Capital Group.

Why the move to Encore Capital Group? "I saw the level of investment they were making in security and that they had a lot of different and interesting security projects going on. It's awesome to be part of that and to help the organization mature." He's energized by the opportunity to accelerate progress: "It's exciting to see how we can continue to grow the security program."

THE PACE OF CHANGE

Konrad stepped into his CISO role at Encore Capital Group with a clear-eyed view of what it takes to modernize cybersecurity programs: understanding risk, staying ahead of emerging threats, and creating a culture of collaboration. "It's an ongoing evolution," he says. "We have to be able to increase with the pace of technology and the threats that are out there."

Konrad acknowledges that while most organizations' business goals tend to remain constant (e.g. increasing efficiency), security must keep up with how those goals are pursued. "We just need to keep pace with the rate of change in technology, regulations and threat actor tactics and what else we need to combat, especially if we're entering another market or changing technology for our core systems."

RISK VERSUS MATURITY

Konrad is pushing his organization to think differently about risk. "Talking about the difference between maturity versus risk, achieving a high level of maturity doesn't necessarily mean you're tackling all of those new threats and risks that are coming out." His message to boards and executives: maturity is not the finish line. It's about aligning controls with emerging risks.

He also challenges the notion of overbuilding: "We don't need to shoot for the Maserati level in each security domain, let's save ourselves some time and effort and take smaller steps that can provide immediate value and risk reduction."

INVESTING WHERE IT COUNTS

In terms of security investments, Konrad is focused on consolidation and efficiency. "As organizations grow and mature over time, they typically collect a variety of disparate tools, so the challenge is how can we reduce those into a fewer number of platforms to drive more effective correlation, efficiency and potential reduction in expense?" He wants fewer solutions doing more work.

One area where he sees a potential to shift priorities across the security industry is identity management. "Identity governance is probably a little overvalued, and where I'd probably focus more is the identity protection space." His reasoning is practical: "You can get a lot more value at a lower cost from identity protection…providing improved, inline protection against identity-based attacks, especially when over 90% of organization are reporting identity-based incidents."

AI, BUZZWORDS, AND BUILDING GUARDRAILS

AI is no longer avoidable, it's operational according to Konrad. He says, "We built a governance process with

governance guidelines for how we onboard any new AI related project. The aim is to make risk-informed decisions and avoid "just leveraging everything that exists."

As for security buzzwords, there's one he's ready to retire: "Zero trust gives a false impression. I don't think it's something we still need to use." He's also weary of the acronym avalanche: "I can't get them straight anymore. It's just way too many, especially when it comes to all the various cloud security products."

BUDGET REALITIES AND RESILIENCE

Even with strong investments in cyber programs, Konrad knows there are limits. "No security team at any organization can expect to have unlimited resources. We must work within reasonable constraints." He urges teams to be strategic: "Maybe you need to change some processes, get rid of busy work, consolidate platforms and get to a more manageable place to drive efficiency."

When it comes to resilience, the expectations are different now. "Executives want to have confidence that we can minimize the impact of a potential breach. That we can detect security events quickly and stop that lateral movement."

CULTURE AND COLLABORATION

Security isn't siloed at Encore Capital. "I get to regularly speak with executive management and the board, so security is always top of mind." What stood out to him immediately was the company's formal risk appetite statement: "Understanding the level of risk the organization is willing to take and what their tolerances are around cyber. This helps ensure everyone is on the same page."

He sees his role as collaborative, not controlling: "We're not the department of 'no'. The way I like to operate is you tell me your problem so I can find a solution that helps you do your job better."