PROFILES IN *Confidence*

MICHAEL BREWER

CISO

NEUROCRINE BIOSCIENCES

Headquarters: San Diego, CA

Employees: 2,500+

Annual Revenue: $2.36 Billion

Michael Brewer's journey into cybersecurity began in the U.S. Army, where his career quickly evolved from running telephone lines to building complex network systems. He shares, "Networking was just starting to become something the Army was going to use for their forward deployed data packages. I attached myself to that team because I saw where the future was going and wanted to make sure, I kept up and had a good career."

That decision set him on a lifelong path of technical curiosity and leadership. He eventually led teams that deployed mobile data networks, gaining early experience in how to secure environments and keep operations running under pressure. "I took a liking to security concepts including different ways of securing an environment, physical and logical, keeping bad people out, and allowing people on site to do what they need to do," he says.

After leaving active duty, Michael started his own company before moving into defense contracting in San Diego, supporting the Navy and various Department of Defense entities. "There's a big footprint here for DoD contractors," he says. "From there I joined as a government employee running the NMCI network as the lead engineer, and later moved to the private sector to do product security for Teradata."

When the pandemic hit, he pivoted again, this time leading pre-sales engineering for a security vendor. During that period, he conducted a cybersecurity assessment for Neurocrine Biosciences. "The CIO liked what I was doing and what I delivered," he recalls. "That was that, I moved over to the Chief Information Security Officer position."

BECOMING A BUSINESS LEADER

Michael quickly realized that being a CISO required both technical depth and business and leadership skills. "There are some skill sets that map well like critical thinking, storytelling, and the ability to condense very technical concepts to a non-technical audience," he explains. "But there were other aspects I wasn't aware of at the time, mainly around legal and compliance for Biotech."

He also discovered that the expectations for CISOs have evolved far beyond traditional IT. "We have to know finance, we have to know the business, we have to know marketing," he says. "We have to be able to articulate cases and tell stories, not only our cybersecurity capabilities but our acumen as business leaders."

BUILDING A MODERN CYBERSECURITY PROGRAM

Today, Michael oversees all aspects of Neurocrine's cybersecurity program, including data protection, identity and access management, security architecture, engineering, governance, and incident response. "It's the entire cybersecurity program," he says. "We also just christened AI security, which I'm sure everybody's dealing with now."

Security awareness is a major priority for him. Michael views it as a cultural issue rather than a compliance checkbox. "People across the business are very smart, but they don't always know the jargon, the risks, or the impact if something goes wrong," he explains. "My goal is to build a culture where people feel comfortable reporting issues. It's not a punitive thing if something bad happens. We need employees to tell us when something seems off."

Looking to the year ahead, his top priorities are risk management, automation, AI security, and maturing third-party risk. "We're a publicly traded company, so we have to deal with audits just like everyone else," he says. "That can take up a lot of time for engineers and architects. We're focused on automating controls and artifacts so we can

standardize the process. It shouldn't depend on who's in the role, anyone should be able to step in and close out that audit artifact."

Michael is also working to gamify security training. "The punitive approach doesn't work," he says. "We're moving toward a gamified, positive approach with department leaderboards and small competitions. It's about getting people to pay attention and making awareness something they want to be part of."

AI, RISK, AND THE CHANGING LANDSCAPE

Artificial intelligence is one of the most significant challenges facing security leaders today. "AI has hit us all sideways," Michael says. "There's no Cyber AI bachelor's degree coming out of school anywhere. There's no formal training because these things, like Model Context Protocol (MCP), just came into realization last year."

"We're learning about these technologies at the same time as the adversaries," he says. "There's really no getting ahead of it. You just have to stay current and agile."

Regulatory complexity adds another layer of pressure. "We have a lot of uncertainty with what's coming out of the current administration," he says. "There's also the state-level piece, and then the global considerations. It's constantly evolving."

That evolving threat landscape requires a balance between security and innovation. "We want to be secure and take a risk-based approach, but the business wants to move quickly," he says. "If we don't adopt new technologies, it can negatively impact the business, but if we move too fast, that can also create risk. Finding that middle ground is the challenge."

LEADING WITH EMPOWERMENT

Michael's leadership philosophy centers on trust and empowerment and he encourages innovation and continuous learning. "If someone goes off and learns something new, I want them to bring it back to the team," he says. "We can figure out together how to adopt it or modify the idea moving forward."

Mentorship has become one of his most meaningful responsibilities. "Helping others grow in their careers is incredibly rewarding. I might only get to work with someone for a small window of their life, but I want to set them up for success."

When hiring, he looks for curiosity and a hunger to learn. "The biggest thing I look for is eagerness, a person who's hungry to learn, self-taught, and collaborative. Everything else can be trained."

STAYING CONNECTED AND GIVING BACK

Michael stays connected to the cybersecurity community through local and national groups. "Here in San Diego, we have many groups, and a small brain trust of CISOs in biotech that meet once a month for lunch," he says. "We just talk about what's going on." He also participates in national industry networks. "These types of groups offer open communication, message boards, Slack channels, all ways to share what's landing and what isn't."

At Neurocrine Biosciences, Michael leads with the same principles that have guided him from the Army to the C-suite including empowerment, communication, and purpose. "Being a CISO is about more than keeping bad actors out," he says. "It's about helping people do what they need to do safely and creating an environment where security enables innovation instead of limiting it."