MIKE TOWERS

CISO
TAKEDA PHARMACEUTICALS INTERNATIONAL

U.S. HEADQUARTERS: Cambridge, MA
GLOBAL HEADQUARTERS: Tokyo, Japan

EMPLOYEES: 52,000+

REVENUE: $32.2 Billion

"I've worked in bio-pharmaceuticals and life sciences for about 25 years and done a lot of work in various IT, digital and technology roles. Working in information security, I've never felt closer to the business. A lot of people across technology functions may sometimes feel isolated. They're not sure where their role may fit within the vision or mission of the company. I don't feel that way at all. I feel deeply embedded with the business and deeply embedded in what we're trying to do as a company. I'm inherently enamored with information security and don't see myself doing anything different," says Mike Towers, the current CISO at Takeda Pharmaceuticals International.

In his previous CISO roles, Towers was the first security hire, building information security programs from the ground up. At Takeda, Towers embraced the challenge of inheriting a preestablished, yet relatively young program. When joining the organization, he saw this as an interesting and exciting opportunity to take a different approach than he had in previous roles. Furthermore, Takeda was about to engage in a large-scale acquisition that would solidify them as a top 10 global pharmaceutical company and Towers was able to leverage his unique experience working in large scale business transactions of integrations, acquisitions and divestitures.

SETTING A STRONG FOUNDATION

Coming into his new role at Takeda, Tower's approach, first and foremost, focused on governance. He explains, "What type of organizational dynamics are in making decisions? What's the overall risk posture of the company? What type of reputation and/or advocacy does the security mindset or function have, whether it's an individual perspective or a collective group perspective? What importance does the company place on security? I spent a lot of time getting to know stakeholders, focused on governance, and obviously spent a lot of time on getting to know the team. Because I was inheriting a team, I wanted to get to know each and every person in the group, not only my direct reports but also the organization as a whole. That was the focus for the initial 30 days."

Towers then began integration planning that involved resourcing and operating model discussions. These discussions included evaluations of staffing, technology partners, service models, budgeting, licensing models, and much more.

After procuring a foundation of understanding, Towers laid out an 18-month strategy. Key to his strategy was benchmarking against peers in the industry. He comments, "I did some benchmarking, and then proposed areas of focus that we needed to concentrate the most on for the next 18 months. It was more of a roadmap construction, then making sure the budget and level of investment that was needed to execute some of those key roadmap items was available. I asked a lot of questions and interjected myself quickly and deeply into the day-to-day operations, so I learned by doing, if you will."

FIVE PILLARS OF FOCUS

Towers has five pillars of focus that he communicates to other business stakeholders as key strategic investment and focus areas for the information security program. These areas ensure the security program continues to make a positive impact on the organization and helps drive successful business outcomes. These pillars include:

Identity management. Towers is shifting focus from internal workforce identity to external ecosystem identity, to include others such as physicians, patients or healthcare providers. By doing so, he ensures these people have a robust identity and access experience similar to that of employees.

Analytics. Focusing on more mathematical and less traditional correlation-based analytics is a top priority for Towers and his team.

Data. For the information security team, focusing on data means understanding patterns of usage and movement, making data a real corporate asset and protecting it properly. Towers is focused on how they make data something that drives decisions, regardless of where it lives.

Product security. Understanding the manufacturing and OT environment is critically important to the security program in order to identify where ongoing protection is required. Towers notes a heavy concentration on OT environments is an industry-wide priority.

Trusted digital experiences. This includes how security partners with the business for enhancements to the digital experience, to ensure the digital landscape is built with the appropriate level of trust and security.

Towers comments, "Those are our five major strategic pillars. They have ongoing focus. I would augment them with a couple of obviously tactical focus areas. The biggest that I'm sure everybody's dealing with is what COVID is doing and how the technology solutions that COVID and the post-COVID recovery are driving to make people more safe and comfortable returning to the workplace. How do you do contact tracing? How do you screen visitors coming into your plants? Among other concerns."

BACK TO THE BASICS

Towers says his five pillars are supported by foundational security hygiene, a critically important element to his program.

He explains, "I think the focus, discipline and behavior I try to instill with my team is never taking your eyes off the ball of basic foundational security. Many well-known and reputable security studies show that a lot of the most egregious and highest impact breaches come in through basic ways. Focusing on foundational hygiene, understanding where you're vulnerable and understanding priorities, is absolutely critical. I'm a big believer in knowing before you control. So rather than diving into things like how you ramp up controls, how you protect and how you apply certain controls, you must know what you have first. Observation, discovery and gathering are important. One of the first fundamental principles of any security professional should be knowing what you're protecting. Your ability to answer that question is very, very important. And I think there's also a very fundamental and strong delineation and requirement to make sure that all this is built into the culture, that these basics aren't unimportant just because they might be older."

Providing Leadership During Acquisition

Before joining Takeda, Towers was made aware of an upcoming large-scale acquisition of another pharmaceutical organization, something he would play a role in during his first few months as CISO. Because he was new to the organization, Towers felt he brought an unbiased perspective during the process of merging the acquired organization's security program with the security program he oversees.

He says, "I got to look at both security programs independently. We did what we call a CARS exercise: continue, accelerate, reduce or stop. We had to make room for some of the areas that were being done that frankly weren't going to add any value moving forward. We took a really good objective look at the program and I appointed my new leadership team within eight weeks of day one. We were able to have some stability in place quite quickly, and then we were able to appoint the rest of the organization within the next month or so after that. I had an opportunity to pull the team together into a cohesive unit very early on."