PROFILES IN *Confidence*

CASSIO GOLDSCHMIDT

CISO
SERVICETITAN

HEADQUARTERS: Glendale, California

EMPLOYEES: 2,500+

REVENUE: Private Company

Cassio Goldschmidt has over 20 years of experience, working across all sized organizations from Fortune 500 companies to startups. He has built security programs from the ground up, positively impacting organizations and strengthening their security programs.

Cassio is currently the CISO of ServiceTitan, a company that provides service visit and construction project software for trade organizations. He has served as their CISO for over five years and continues to enjoy his work because of the strong organizational leadership in place and commitment to cybersecurity. Cassio says he joined because of the mission of the organization, built by two individuals who identified a lack of technology in an underserved industry. The company had about 600 employees when Cassio started and now has over 2,500 employees, something he attributes to their strong culture.

When joining the organization, Cassio was technically the first hire in security, although there were security efforts from the engineering team before he joined. He explains, "There was no central security team before I joined, so I was responsible for a completely blank page. I was focused on building the team, figuring out who we needed to hire, identifying the first projects that we were going to tackle, and understanding how to communicate and interact with all the other teams. And quite frankly, this can be very scary for a lot of CISOs. But because I've built programs from the ground up before, I had a good blueprint of what to execute. However, I always make sure that when I'm building a program, I aim to create a replica of what I've done in the past; instead, I tailor it to the company I'm working for and their specific needs."

FOCUSING ON STRONG COMMUNICATION

Armed with a Bachelors in Computer Science, Masters in Software Engineering, and an MBA, Cassio felt prepared to help ServiceTitan grow and strengthen their security practice. Not only did he need to ensure the right security processes and procedures were in place, but he also knew it was vital to solidify strong relationships with executives and employees across the organization. This was important in order to gain key buy-in and build awareness about the security program goals and projects.

He comments, "When communicating with upper management, it's important to understand the technical side, while also understanding the needs of the business and not only the executives that are running the company, but also putting myself in the customer's shoes, working with sales, working with customer support, and so on. This helps give assurance that I will be focused on making sure our customers have peace of mind when working with our organization."

He continues, "Something I found interesting when I started hiring was that my first team member was somebody with information security background and also an MBA. And the next hire also had an MBA and was somebody with a technical background. That is incredibly rare, but I think that was a huge advantage for us in order to have people who were not only technically savvy, but always knew how to talk to the business."

The most important thing to Cassio was to build a culture of security that includes executive presence and influence. He relies on connecting with people and educating in a way that helps them understand the importance of security. He says, "You have to use empathy and appeal to the emotional side of things, and also show that you are not doing this because it's your own agenda. It's really all about the company goals and priorities, and to show that you have nothing but the best intentions in mind. It sounds super simple, but it's really hard to create those relationships and bring people to your side, and create this culture in the first place, but that is the number one thing that all CISOs should be doing because as people say, it takes a village."

"I've worked in my teams' shoes. I love to listen to people because their work is always changing. And understanding, listening, and knowing that they have a voice is very important."

CURRENT INITIATIVES AND INDUSTRY TRENDS

Cassio's current initiatives include full verification of machines and identities and right sizing privileges. Cassio says the days of having different roles and different tools is coming to an end and we are going to see more of right sizing privileges, meaning dynamically providing privileges based on needs and looking at logs to understand what kind of privileges people had and didn't use.

Another area of focus is around acquisitions and ensuring there is technical and procedural alignment between ServiceTitan and any organizations they acquire. This means expanding services to the acquired organization with things like their Bug Bounty program. The biggest focus in any acquisition is keeping security consistent to make sure practices, tools, and other areas are effective and properly covered.

In general, for the cybersecurity industry, Cassio sees access to tokens as something to look out for. He explains, "Instead of stealing data and terabytes going through routers and so on, these days if somebody gets an API token and copies it on a piece of paper, it doesn't even pass through your DLP. A former employee or attacker can get a discrete amount of data on demand as long as they want, especially if you know the tokens are not properly refreshed, or API queues are not properly rotated. So as people move to the cloud, you see more and more of these kinds of interactions using machine to machine credentials or API tokens and so on. And I don't think most of the CISOs actually see the problem with that."

Another relevant trend in the industry is Artificial Intelligence (AI), something Cassio has been studying and has been up to date on for many years. He has published articles on the topic, talking about generative AI and how it impacts business, and written papers on AI and the risk for business, to name a few. Cassio attends conferences on a regular basis, many with tracks or focus areas on AI that he chooses to actively participate in. He also received an AI certification from Microsoft. It is important he stays up to date on AI because of its impact on the cybersecurity industry. By self-learning and contributing to the community, Cassio not only educates himself, but he also spreads his knowledge with the broader industry of security professionals.

He comments, "I think AI has potential to become a big headache, especially with attacks such as business e-mail compromise. If AI understands the entire communication going on between two people, it can get in the middle of this communication and start acting as the person you're communicating with. None of the solutions we have out there are going to be able to detect these kinds of things properly. But there's also a lot of things that AI is going to help us prevent. And I think it's really a great thing that came to the industry and will help us tremendously in the future."

LEADERSHIP

Cassio prides himself on providing his team autonomy and the ability to speak up and contribute their own ideas. He comments, "I've worked in my teams' shoes. I love to listen to people because their work is always changing. And understanding, listening, and knowing that they have a voice is very important. Building relationships across business teams is also very important. It's really important to build those bridges not only internally, but also externally, speaking in conferences, collaborating with the community, which I try to do as much as I can. I can really bring the best back to the company and help the team grow. I am always focused on our people and that they get the education they deserve."

To keep growing on a personal and professional level, Cassio engages with all aspects of the cybersecurity community. He talks and meets with other CISOs at many industry conferences and has created a strong network of collaborators amongst his peers. This helps him address challenges, discuss industry trends, and continue to learn from people who are going through the same experiences he is.

Cassio also works with startups and VCs to expand his knowledge and learn from new-to-market security companies. He says, "There are a lot of startups, they're very innovative and they're doing things differently in solving problems that big companies have been focused on. When you talk with a startup and you become part of their customer advisory board, you can influence their solutions in order to work in your type of environment. I spend several hours during the week talking with startups and also VCs."