PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

MAARTEN VAN HORENBEECK
CISO, ZENDESK

HEADQUARTERS: San Francisco, CA

EMPLOYEES: 2,000+

ANNUAL REVENUE: $500 Million

"There's always ways to deal with the threat of the day, but in the end, you need to build a culture that's agile and open enough to using those technologies and using the different people in the organization to help protect the organization."

- Maarten Van Horenbeeck

Originally from Belgium, Maarten Van Horenbeeck began his career as a security engineer, splitting his talent between his day job and voluntarily helping nonprofits with their security needs during the evenings. Stemming from this early work, Van Horenbeeck gained perspective on how to implement security and realized security was much less about a technical problem, and instead more of a problem of culture. He recognized the importance of building a culture of security within an organization to be effective. He says, "There's always ways to deal with the threat of the day, but in the end, you need to build a culture that's agile and open enough to using those technologies and using the different people in the organization to help protect the organization."

In the late 2000s, Van Horenbeeck worked at Microsoft as a manager who helped release security updates for the Windows platform and protect users of the operating system. The main challenge for him was building security into Microsoft products and creating a culture of security. After other high-level positions in information security, Van Horenbeeck joined a startup company where he built out the security capabilities from the ground up before moving into the CISO role at Zendesk.

GROWING INTO A CISO LEADER

Six months ago, Van Horenbeeck was hired as CISO at Zendesk, a cloud-based help desk solution offering customer service software and support ticketing systems. When discussing the growth into a C-level executive, Van Horenbeeck describes it as a transition of learning to 'let go.' He explains, "For me to transition from being an engineer to a leader has really been about letting go. It's been about identifying the areas where I was no longer the best person to do this job and figure out how to hire, retain, and get those people on board that are the best people to do that specific work. It is something I've personally always had a challenge with. In fact, I like to be in an organization where I can still step in and do something when it's necessary and as you grow into a chief information security officer role, you must accept that you're no longer in that place."

When discussing his role and what it means for handling risk, he believes it to be one of the biggest differences in becoming CISO. He says, "When it comes to assessing the risks, the buck really does stop with me. I have to bring together the views of my team. I have to bring together the views of other executives and identify what risk is appropriate for us as an organization and what isn't and be sure that we communicate very transparently and very openly so the business can actually make the right decisions."

THE IMPORTANCE OF A SECURITY-FOCUSED PURPOSE

"We came up with what our purpose is in the organization, and I like the term purpose over mission because when you have a mission, it implies that there's an end to this. It's important to note that when you have a mission and you fail, people will be very disillusioned. I'll give you an example. If you have a mission to protect the enterprise from a breach and you have a breach, then you effectively fail at your mission and people will feel disappointment with the work that was delivered or what was done. The important thing to acknowledge in security is that you will never get everything perfect," says Van Horenbeeck.

For Van Horenbeeck and his team, having a sense of purpose solidifies their core goals of protecting the company, customers, and employees from threats. Even if an incident occurs, his team still uses their purpose to take the right action items to make sure they protect data or people to the greatest degree they possibly can. The goals supporting his teams' purpose are building a security culture, ensuring effective prioritization, supporting business decisions, and becoming a learning organization.

"My main goal is that we do things that are repeatable. We must be consistent and make sure the teams understand why we do what we do, and that leads to a level of trust that allows them to interact with us more effectively. We also need to understand where we are today, what our gaps are, and how we can reduce risk. We need to understand what that risk is, communicate it effectively across a wide set of individuals, both at a technical level and executive leadership level, and make sure that we can help them drive the right business decisions to balance that risk against growing the organization or doing great things for our customers," states Van Horenbeeck.

When discussing risk with executives, Van Horenbeeck recognizes everyone has a different boundary of how much information they are interested in. As a CISO, he describes the importance of starting higher level and conveying critical facts, but also understanding how deep to go with each individual. He says, "It is a little bit of an individualized approach depending on the leader that you're actually working with. And I think sometimes it's a mistake to start off assuming they all have the exact level of information they require to make a solo decision and feel comfortable with the decisions that you're recommending."

STRATEGICALLY APPROACHING CHALLENGES

In a recent meeting, an employee asked Van Horenbeeck what keeps him up at night as a CISO and the biggest threats facing Zendesk. He replied with an unexpected answer by revealing his greatest concern was being able to hire and retain great people. He explained how everything in security starts with good people who can help move the needle. While hiring in security has become incredibly challenging, especially in the San Francisco area, it is vital to create an environment where people want to work and where they can apply their passion to protecting the company, employees, and customers.

A second threat Van Horenbeeck sees is the different boundaries between where companies inter-operate and where customers inter-operate with those companies. He explains, "As a SaaS provider, one of the big things we do is invest a significant amount of our time building a secure product, and that means addressing software vulnerabilities. There's a boundary there between how customers use the product and it's sometimes less understood these days with how quickly the internet and SaaS services are growing."

Putting Customers First

"When we built out our security program, I tried to take the philosophical approaches we have in place and distill them down into what we do as an organization to be effective. And the single most important one for me was when I joined Zendesk, we always put our customers at the center of what we do. And that's something that we really tried to replicate in the security team, it's something that just intrinsically makes sense to all the employees, so it was a nice framework we could use to tell them how we see security. Some practical ways that we put that into place was by making sure that we push knowledge to our developer and engineering community so that they can actually make security decisions without always having to come to security."