DAMIAN CHUNG

BUSINESS INFORMATION SECURITY OFFICER

NETSKOPE

HEADQUARTERS: Santa Clara, CA

EMPLOYEES: 2500

REVENUE: Private Company

TELL US ABOUT YOUR ROLE AS CISO NETSKOPE?

My main role is to run security operations for Netskope internally on our corporate side. But as you know, I'm also a practitioner talking about how we see security in the future and trying to drive operational efficiency within security operations. As such, I also work in a customer-facing capacity, in addition to my primary role. While I'm not part of the sales organization or the sales cycle, I should point out that I do run our product as one of our core tools, but also integrate that with a lot of other security products in our stack. This affords me the opportunity to honestly and authentically go out there and talk about our experiences, best practices, and how to drive efficiencies and business value from our internal security program.

FROM A SECURITY OPERATIONS PERSPECTIVE, WOULD YOU SAY NETSKOPE RUNS THAT PROGRAM SIMILAR TO ANY OTHER NON-SECURITY ORGANIZATION?

Before working at Netskope, I was part of a large security team with 60,000 total users across the enterprise. So, running a security program like that, as you can imagine, is a lot bigger, but it's very similar. The difference with Netskope is they don't have a lot of legacy systems. We're very cloud-forward. Thinking about how we deploy security across that type of platform, four years ago would have been a challenge, but today it's different because of better tools. It's not like we need to be scared of digital transformation anymore. Security has always been known as the "Department of No". But what we want to do is promote security as a business enabler, so the only difference is that I can be a little bit more strategic and cutting edge, and I want to say take more chances, but in reality we're not taking more chances. We are pushing the boundaries of how we think security should be in the future and leading by example, not just talking about it, actually doing it and then publishing best practices.

HOW DO YOU ENSURE SECURITY IS PART OF THE SDLC?

It's part of building the culture, really. SDLC is huge for us. Just trying to make sure that our product itself is developed securely, takes a lot of culture and education. One aspect is that we have a "security warrior" program where we're instilling that kind of culture within our developers so they are doing the best practices according to their software development and making sure that we are testing that through our own internal red team and purple team against our own product. For companies that don't develop their own products that might be new to them, but for us it's a major part of our program.

HOW DO YOU APPROACH THIRD-PARTY RISK?

We go through frameworks and get the certifications that give us some standards to work toward, and if our customers are asking us questions on how we manage our security, we can point to some of those certifications. We also have a dedicated GRC team that can answer questions on how we handle our own data, our customers data, development of our code and even business resiliency for the product, because a lot of customers are depending on us. I look at third-party risk as trying to understand my vendors because we are on both sides of this; I have to be a customer of other vendors as well.

I'm worried about protecting my organization and our data through potential issues with our third-parties, and so on the flip side of that, we are a third-party for our customers and they have the same questions. So, because we're in between, we play both sides of that. I totally understand the importance of making sure that we hit our compliance, making sure that we are up to date with our security and vulnerability management and making sure that we're communicating those with our customers so that they're aware of how we're addressing zero-day vulnerabilities and trying to make sure that we hit our own SLA's in terms of patching and remediation.

HOW ARE YOU THEN COMMUNICATING THAT WITH CUSTOMERS?

At Netskope, we treat our customers as partners. If they have a question, we have a whole GRC team that can answer anything about governance, risk, and compliance. We have a very strong community online where a lot of our customers can ask those questions as well or just email us directly. If there's a major vulnerability in a tool that we use, we will let them know whether we're using that tool or not. It may not be something in our environment, but we will still send an email to our customers letting them know this is not a tool that we use within our environment, so the vulnerability does not affect us. Or if it is a tool that we're using within our environment we tell them that we've successfully patched it and we've covered it. A lot of that communication is really, really important, just to give the customers peace of mind. Because if you don't communicate with customers, they just don't know where you stand, and they don't know what the status is for any kind of issues that may come up throughout the lifecycle.

HOW DO YOU EFFECTIVELY COMMUNICATE WITH EXECUTIVES AND THE BOARD?

Our entire organization is generally more knowledgeable on the cybersecurity front, but we still have to do a lot of communicating across our organization because they may not be up to date with what's going on today for specific attack vectors, for the broader organization. We do have people looking at threat intelligence and recovering that for our customers like any other organization. When I go to our executives, do I need to go and justify purchases? Absolutely. Even for our own products, so I do operationalize the Netskope product within Netskope. That's one of our core programs.

We look at the business value of all of our tools. Every year we'll take a look at the tools we have in our security stack, evaluate them, and also review our total spend across our program. The communication to our executives still has to happen in a way that they understand how we're operating and the maturity of our security program. But it's not like I get a blank check to purchase anything that I want. We don't get to just blindly go out there and implement tools, because at that point you would become inefficient in your security program. You just have tool fatigue, alert fatigue. So, it's a matter of presenting your program to executive leaders so that they understand the business value of the security program. And that is applicable to us on the vendor side as much as it is on the customer side.

DO YOU THINK YOU SPEND MORE ON SECURITY INTERNALLY THAN NON-SECURITY ORGANIZATIONS?

It depends. I don't think I could say yes or no. There are probably customers that spend more per employee on security than we do, and then there's probably a lot that don't spend enough or a lot less than us, so I couldn't really answer whether we spend more or less. It just depends on what vertical, who they are, and how advanced they are. Are we well-funded? I would say yes. Do I have an unlimited budget? No. Do we have a good handle on some of our business use cases and communications with our executives? Yes, we do and that's because we are a security company, so it is a high priority for us to make sure that we have a mature program. What we don't want to do is spend and spend inefficiently. You can't solve a security program by just buying tools, and I think we've addressed that. We want to be able to show that we're part of the business and we are enabling them and spending our dollars wisely.

As I said earlier, we don't get unlimited spend, but we do get funded sufficiently. And if there's a major gap, it's really about communicating what that risk is and doing an evaluation based on how much that remediation would cost versus the risk.