DENNIS DAYMAN

RESIDENT CISO
PROOFPOINT

proofpoint.

HEADQUARTERS: Sunnyvale, CA

EMPLOYEES: 4,500

REVENUE: Private Company

WHAT CONVERSATIONS DO YOU HAVE WITH CUSTOMERS?

The team that I am on is called the Resident Chief Information Security Officer (RCISO) team. Many of us have been in the security arena as CISOs for a long time—and like me sometimes for 30 plus years—so we have a good deal of operational experience. Within our company, this allows the RCISO team to drive and support our people-centric security vision for our clients. Whether they need to understand current cybersecurity trends as revealed in our annual Voice of the CISO and Board of Directors reports, require assistance with account team strategy, or have a customer CISO requesting support for a business case, we are here to help.

The company even has a Customer Advisory Board (CAB) that we meet with regularly to understand their concerns, problems, and what they're seeing in terms of security issues. We share what we've learned in instituting technologies like Proofpoint, and how we would do it from an operational CISO role at those companies.

When talking to customers, I always want to know what's keeping them up at night. And for a lot of them, they're not sure which direction to take. If they come to us and work with our team, but also allow us to listen to them about what technologies are out there and what has not worked in the past, it helps us build a better product and improve customer service for defending their data and protecting their people.

It's going to get even more interesting over the next couple of months, because we're expecting a new rule from the Securities and Exchange Commission (SEC). The SEC is now saying they'd like to see a CISO on the board of publicly traded companies because they want that board to be more aware of what's going on. And also, to put some accountability into what the board may or may not be investing in from a security perspective.

What we're doing from the RCISO program is to bring in as much insight from all over the place, as our team consists of people who have been in healthcare, financial services, and SaaS based technology companies. And this breadth of experience is great as a group because we go and speak at events. We go and listen to understand what have we not been seeing, what have we not been hearing and how can we spread that information too.

WHAT IS MOST IMPORTANT WHEN COMMUNICATING WITH CUSTOMERS?

Number one, hyper transparency is most important. Not hiding behind the issues or the terms and conditions. The Customer Advisory Board is one way that we communicate work with customers. As we're developing new technologies or we're seeing the threats we want them to be aware of, we are always as open and candid as we can be. This is number one for me.

We do a lot of roadshows and go and meet with customers. In fact, over the last couple of weeks, I've been traveling and meeting some of our own partners as well, talking to their customers about what's happening in the world, hearing what they are seeing in their own companies, what's out there, sharing what data policies are and how to implement them with technology. I try to be open and share that with as many people as I can.

HOW SHOULD ORGANIZATIONS PROTECT CUSTOMER DATA?

It really starts with people. We know that you have to defend the data, but you also have to protect the people. And in today's world, a lot of threat actors are not necessarily going after systems anymore. They're going after the VIPs, if you will, the privileged access accounts (PAM) that are out there. And the best thing you can do right now is to build tools and invest in training to help people protect themselves and be better prepared. If you put the right tools into their hands like looking for malicious URLs where they don't really have to always think about it, they still need to be trained on it. But showing them that by looking at a URL and seeing misspellings or looking for misspellings within the domain that the e-mail might be coming from, that's where it really begins.

HOW DO YOU DISCUSS BUDGETS WITH CUSTOMERS?

Customers are naturally concerned about budgets. They do come to us and say — 'okay, how are we going to show that there's going to be a benefit from this?' And we're able to do so with a lot of different tools and methodologies that we've created with customer input. At Proofpoint, we have business case studies that greatly help them show value.

We actually sit down, trying not to oversell them to begin with, as we know a lot of companies want to sell them everything under the umbrella, not necessarily what they need right now. Maybe you might need some things a little bit later and that's fine. Let's start with the most pressing issue right now so that we can make that budget hit a little bit easier, and then move into that flight of products.

We create these business cases not only for the buyer, but for them to be able to give that to their board and their business unit management. They can then show that by not implementing these sorts of technologies, if there was a data breach it would cost them a certain amount of dollars. But by instituting this technology, person by person, license by license, technology by technology, this is really what we're going to save in the long run by investing in it now, and over time as we need, we can then add on more as we see fit.

HOW DO YOU ADDRESS THIRD PARTY RISK?

A lot of companies unfortunately still don't regularly meet or work with their third parties. It's almost like a sign and forget it sort of contractual effort. You're going to go off and do an audit, then internally, why aren't you running those sorts of audits with your third party? Even from a contractual relationship, what sorts of things are you requiring to do in privacy?

I was also a Chief Privacy Officer. We always talked about the principle of "data minimization," meaning that a data controller should limit the collection of personal information to what is directly relevant and necessary to accomplish a specified purpose or only holding on to the data, using the data for the time that you need it for, and then getting rid of it. If you're working with supply chain and third parties, make sure your third parties are also reducing the amount of data they're holding onto during a specific time period. Make sure that they also meet your own internal policies when it comes to data minimization.

If you've got a policy for a specific thing within, say finance, maybe they should be also meeting that same threshold, whatever that policy could be in data holding time periods. Again, most companies go off, they just sign an agreement and that's it, they never regularly review their third parties. They assume it will make their systems work better, but they have to function the same way you would create or force your own people within your own company.

HOW DOES YOUR WORK AS A PRIVACY OFFICER IMPACT CONVERSATIONS WITH CUSTOMERS?

When you look at what's happening just here at the state level to begin with, we're seeing many more states now coming up with new data breach regulations.

We have about five states with privacy regulations. There are about 52 bills out of 24 states that are being pushed through with all sorts of fines and misuse of data or data being breached. The cost structure is going up. You look at what happened with GDPR once it came out. Being able to fine you a certain amount of your firm's annual revenue from the preceding financial year, you look at that and realize you don't want to be the next example of a fine or loss of trust from PR issues that have untold losses associated with it.

We are also seeing insurance companies not paying out policies when companies have a breach. They are not paying out because when they investigate the case, they find employee malfeasance or employees doing something incorrectly, and they can prove it which invalidates the policy. They say, 'sorry, your policy doesn't pay out for misuse or not having the proper security. So, you're on your own now.' They pull in products like ours to then hopefully be able to get another cyber insurance policy.