RICHARD BIRD

CSO
TRACEABLE

HEADQUARTERS: San Francisco, CA

EMPLOYEES: 150+

REVENUE: Private Company

K LOGIX PARTNER PROFILES

HOW WOULD YOU DESCRIBE YOUR ROLE?

Being a CISO at a security solutions company like Traceable is a dynamic role. I am an evangelist for security innovation, security best practices, and the functioning CISO for both internal corporate as well as product, and that takes up about 30% of my time. I am lucky that we have a really great security staff that does all that heavy work. I get involved in any incident reporting and managing the security team. Before transitioning to a dual role about 5 years ago, I spent 20 plus years on the corporate side. I'm not only someone that's been a CISO, I'm someone who has also been a CIO. I came up through IT operations in the first half of my technology career, then I moved into cyber security for the second half. What is awesome about my role is I get to help grow a company, be an influencer driving innovation and coach and lead others on a hard core security team.

About 70% to 80% of my time is customer-facing with other CISOs around things like strategic program creation, like "Why should I buy an API security tool? How do I establish the criteria for buying the right API security tools? What else do I need to do?" This is really new ground everywhere because I have seen this pattern before.

I used to have data governance problems. I used to have IT asset management problems. I didn't know how many things I had. I didn't know how many firewalls or how many firewall rules I had or how many virtual servers I had. So a lot of my conversations with colleagues and peers in the enterprise world are regarding – How do we frame up governance around API security? How do we frame up ownership? Which organizations should actually be responsible for it? All those kinds of mechanics and that's where I get to leverage my 20 plus years of experience, building those programs and helping CISOs and CSOs that have tremendous responsibility in enterprise space.

HOW IS TRACEABLE ENSURING THEIR CUSTOMER DATA IS SAFE?

The way that we ensure customer data is safe, is by providing customers with the ability to never let us have their data, at least not in its raw form.

We provide, as part of our feature and functionality capabilities, the ability for customers to obfuscate any sensitive data or all data that they want to. When you implement Traceable, we typically implement it with obfuscation rules that meet compliance requirements that meet current data privacy standards, like GDPR or the California Consumer Protection Act.

Traceable never actually sees any real data, and that provides a certain amount of comfort for organizations that are trying to maintain strict data privacy. An alternative for highly regulated customers that say 'Wow, APIs handle critical information. There is competitive operational intel that can be derived from all the things that APIs do from a tracing and monitoring standpoint. I really wouldn't like that sitting in your cloud solution. I'd actually like it if you just gave me the software and I installed it.' So we provide both an on-prem and a SaaS solution. And once again, either way, we never see any raw data, we take the whole issue of data confidentiality to heart and that's the way we've designed the application.

HOW DO YOU ADDRESS THIRD PARTY RISK?

Most supply chain attacks are executed through APIs. Being an API security organization, we have the capability to monitor our own systems, monitor our own transactions with our own tool set.

We're able to see the activity that's going on, where there is connection between endpoints, connection between applications, in a supply chain between suppliers, between third party providers, and see exactly what's being done nefariously.

We basically were built to be part of the solution set that reduces supply chain risk and shrinks the attack surface. Traceable is fortunate that we're in the business of securing the major pathways and the connection points that are currently used for supply chain attacks, so it's something that we are just sensitive to on a day-to-day basis because we are monitoring for any kind of bad outcome across billions of calls every month.

HOW DOES TRACEABLE APPROACH THEIR SPEND ON INTERNAL SECURITY?

I would say that if we were comparing to other companies that are in our stage of growth, of a round B funded startup, I would say that our security spend is probably slightly above average for security solutions providers in our space.

And the reason for that is because, like I said, so many aspects of what we do are tied to key security concepts. Zero Trust is a great example, as well as the supply chain. And since we're a security solution that helps mitigate risks in those spaces, we're probably applying more dollars towards product security and operational security than most of our peers.

But again, we're shoemakers, and everybody wants our shoes, but we also wear our own shoes because we're just in the midst of a transactional layer of security that requires us to be a little bit more rigid around our own security practices.

HOW DO YOU DETERMINE WHAT SECURITY TO PERFORM IN HOUSE VS. OUTSOURCE?

That's tough for all startups. The reality is that I'd love to say that we could go and outsource the assessments necessary, or other certifications such as NIST or ISO certifications, and FedRAMP certifications. But there are investment dollars that are associated with that, and the challenge is that most companies in our size and class don't have the available resources or experience.

And yet when we go to have conversations with external sources to do that work, it's not inexpensive. It creates a really challenging problem for us, in that we have to choose which security assessment credentials are most important to your buying customer.

They would love for us to have all the certifications, but I think the buying population also recognizes the problem in this space, that these certifications require investment dollars that need to be leveraged for other aspects of the company growth, until we reach a certain phase where, being able to pay for them makes sense with in house or outsourced resources depending on the skill and expertise required..

HOW DO YOU APPROACH CUSTOMER COMMUNICATION?

Many of our security interactions and security communication tend to be associated with making sure that we're on the right security footing to be a third party solution provider to enterprise companies. We're a relatively new start up, having come out of stealth less than two years ago for the most part. We're SOC2 certified and we have to go through really rigorous security assessments.

We also have an Advisory Board where we take inputs from our customers around security topics, that we are either addressing them as it relates to operational security, or having conversations about them in relation to product security in future features and functionality requirements for the roadmap.

In addition we have a customer success team that is always interacting with customers to improve the nature of all our interactions with them, including communication and improve product performance and capabilities.