# TIM ROHRBAUGH

**CISO**
**JETBLUE AIRLINES**

**HEADQUARTERS:** Long Island City, New York

**EMPLOYEES:** 22,000+

**REVENUE:** $2.95 Billion (2020)

Tim Rohrbaugh began his career on the aviation side of the Navy, working in secure communication in the late 1980s and early 1990s. In his next role, he worked on projects related to air defense and Information Assurance and split his time teaching a course on securing systems at The Defense Information Systems Agency, enabling him to see both the practical side and the compliance side of security.

After moving into the commercial sector, Rohrbaugh worked in financial services as a CISO. He comments, "We gave consumers the first view of their credit file by bridging the three bureaus and then writing a contract with each of them to provide credit data to the named individual. We had to solve challenges like ID verification (having people prove who they say they are), some of the modern authentication schemes and the beginnings of what was to become the privacy sector. It was a very interesting time. I also spent six of those years on the board of the Online Trust Alliance where it gave me a view into the regulatory challenges, and I specifically looked at influencing what was, we hoped, national legislation around privacy."

He then worked for a compliance firm where he ran North America consulting services before they were acquired. After this, Rohrbaugh began his own virtual CISO company with JetBlue as a client. He took on an Interim CISO role and was shortly hired for the full-time role.

Rohrbaugh explains, "I stepped into JetBlue with a three-month Interim CISO contract and after about one month we found that it was a really good match between us. And they asked if I would apply for the permanent CISO role which started in late 2019. I think for me, I had almost forgotten how much I loved aviation because I had been out of aviation for a while. Being back in the middle of it and a strong positive culture like JetBlue, valuing passion and kindness, was exciting to me. That is what I found very appealing and unusual in today's commercial sectors."

He currently reports into the General Counsel and sees a strong benefit in this reporting structure. He finds it conducive because legal is focused on mitigating risk associated with compliance and regulatory, and Rohrbaugh and his team work to mitigate risk from a security perspective.

He says, "From 2003 to 2006, I reported to the CIO, the CEO, the COO, and then I moved under the General Counsel, and I found such a nice match of our objectives and also sometimes how we've characterized risk within the company. Everything that a CISO requires of IT is going to cause some amount of tension because it's going to add time to development, it's going to add labor cost, so we have to be very judicious about exactly what we're asking of them to do and doing it outside of the CIO reporting structure incentivizes both teams to work in a very cooperative fashion."

## DEMONSTRATING VALUE

Like many security leaders, Rohrbaugh acknowledges the challenge of justification and leveraging a set of metrics to reflect progress and value of the security program. He believes anything presented to a Board or executives must be carefully curated to match the specific context of security risk for the organization. These could include technical and business requirements, controls, and objectives, to truly understand what the organization would benefit from, all from a risk reduction standpoint.

He explains, "I was brought up under the waterfall methodology. Unfortunately, many times we started and it took so long to complete a project, by the time we were done we chose the wrong technologies, or worse sometimes the mission changed. And once I was introduced to the Agile, I really fell in love with it as a product owner. I was also head of a product in the past, which is unusual for a CISO, but that experience was impactful in the way I look at security program improvement. I can tell you what I've tried to do is change the way security programs improve by focusing in on change in a way that's more akin to Kaizen - smallest change possible. What is the smallest change you can make that is going to improve security? And many times that means doing so by frustrating the criminal, by making it slightly more difficult, by giving you just a little bit more visibility. If you break down that work and improve the security posture with even four hours at a time of effort, effectively what you end up doing is avoid making big bets in one direction and knowing full well that criminality changes on a dime. Instead, we make a change, hypothesize how that's going to influence, then measure it and see if it does. And if it does not, well you did not invest that much time going the wrong direction. Instead, we try a different way. As a benefit for team members, no one is pigeonholed, as there is a chance for everybody on the teams to self-select based on the areas of the domains that they are most passionate about. And for the most part, they really enjoy it. I hope to tell you more about how it works out in the future, but right now all signs look that it's a good approach."

## TECHNICAL DEBT AND NEW INVESTMENTS

Rohrbaugh says the airline industry is currently in a period of rebuilding since most airlines recently experienced significant budget cuts among other changes. In this moment of rebuilding, there is a significant amount of technical debt that exists.

He explains, "Every business is trying to adapt. As they are adapting technology, you make choices and sometimes when you try to actually produce the features and functionalities that are requested by the business, you take shortcuts, or you take solutions that may not provide the visibility from a security perspective. Maybe the visibility that you need into the transaction details to determine if something is normal or abnormal falls short. Sometimes we use technologies that may constantly require updating because they're being attacked or found flawed, whatever it may be, those choices are generally not the ones that you would make if you had enough time, or if you had timelines that were reasonable. So all of those little choices, which are not conducive to stopping misuse or preventing discovery or whatever it may be, must be addressed post release. Meaning, you must go back and clean those up. Technical debt is sometimes development, sometimes systems, sometimes features other times visibility. Right now, as we try to compete with required changes for the business such as new features and functionality, we have to sequence in some of these cleanup activities."

When investing in new products, Rohrbaugh believes the security product marketplace is filled with misconceptions and miscommunication. He comments, "I don't want to be constrained when I'm thinking about a solution to a bunch of checkbox features that were identified by X. I specifically don't like to see those marketing terms in any communication or sales pitch, I like product owners and sales staff to talk about what they're doing, why they are doing it, and what value they bring. But beyond that, for me it starts with humans, the people are how you solve the most complex problems, there's no product that's going to compare with the cognitive ability of a trained analyst. Yes, they might be able to react faster with automation, but you still need the experts to actually program or influence some of those rules."

### IDENTITY

With his background working in the financial space, Rohrbaugh has keen experience around identity and says many people may struggle with understanding the difference between ID verification and authentication. He explains, "You have to have some amount of confidence in the person you have actually created the account for. They must prove they are who they say they are. Authentication on the other hand comes after this step, then you need to capture enough data on them so you can test later. You then have to exchange some mechanism for them to log on successfully with you."

He continues, "The techniques that we use today, with respect to ID verification are pretty strong in specific sectors e.g. the banking sector, but if you keep reusing these tools in other ways, you de-value them. I found in the past that somebody could go through an ID verification, and you would find that a criminal could pretend to be somebody else taking the test faster than the actual individual. And so you could almost pattern that it's more than likely fake or fraudulent, the faster the test, which is counterintuitive."

Behavior analytics is underutilized yet considered a key component of account monitoring according to Rohrbaugh. By having a strong focus on patterning normal and abnormal behavior, Rohrbaugh believes criminals will be more challenged to steal an identity or account and first determine what is normal behavior and operate in the confines of this normal activity, or risk being discovered.