DWAYNE STEINWAY

CISO
AUDACY, INC.

HEADQUARTERS: Philadelphia, PA

EMPLOYEES: 4,000

REVENUE: $1.46 Billion

Dwayne Steinway began his career in the Navy as an Intelligence Specialist, where he worked in IT with some aspects of security-related work. After leaving the Navy, Steinway was recruited to a consulting organization, where he was introduced to security practices within the consulting ranks. He had the opportunity to begin working on firewall and security infrastructure projects, with the rest of his security career blossoming from there.

After working in a variety of security roles across different verticals, he joined Audacy, Inc. in 2020 as their Chief Information Security Officer. Audacy, Inc. is a scaled, multi-platform audio content and entertainment company. Steinway explains, "I came to Audacy essentially as their first formal security leader. For nearly 20 years, I managed security teams across different industries, but never audio. Audacy came forward with this position and I saw that it is a very technology-rich organization. There is a lot of unique infrastructure here that you do not see in many other industries. It became a really appealing opportunity for me to dive into a new industry and apply the familiar trade, but in a new way."

His main responsibilities include the traditional security operations functions of threat management, risk management, and compliance. He is responsible for incident response activities, managing both the incident responders within his security team and externally, evaluating threats and addressing any security issues. DevOps and cloud infrastructure also fall under Steinway's responsibilities. He comments, "We have a large cloud infrastructure that supports our audio distribution infrastructure and other related applications. I am responsible for the digital infrastructure team that manages those environments in the cloud. It's a relatively new thing for CISOs. I know some CISOs who have an indirect responsibility or a close connection to DevOps. I am actually directly responsible for them. So, I have SecOps and DevOps under me, in addition to the compliance functions that come with being in the CISO seat."

SETTING STRONG SECURITY GOALS

Security hygiene is one of Steinway's top focus areas, because the infrastructure is fairly diversified across Audacy's 47 markets and the cloud. His team works on unification under one security program. He says, "Every market has a team of experienced engineers, and in each market they're responsible

> *"...our goal is to make sure that at the very least our security practices are normalized across the markets, where we are seeing the events the same way, regardless of the technologies that are in place."*

for those stations that they support, and they may have different preferences for the mix of technologies they like to use to manage that. So we have a variety in the technologies that support the business operations. For our security program, our goal is to make sure that at the very least our security practices are normalized across the markets, where we are seeing the events the same way, regardless of the technologies that are in place."

Another goal is ensuring operational practices follow specific security guidelines, and making certain that operational work, and especially enhancements, support the organization's overall security strategy and expectations. He explains, "That's why the DevOps integration has been crucial for me, because now I can understand and help in the development cycles, and ultimately support the need for better threat monitoring and secure code reviews for example in the places and pipelines where they make the most sense. I could be the one to advocate for these, and even go to leadership and request the funding to do it. It is a little easier when I am directly involved with the team. I would say it has been beneficial relationship both tactically and strategically."

TALENT, BUDGET, AND VISIBILITY

One of the most significant challenges for Steinway, and most other security leaders, is talent. He said he struggles to find replacements if someone on his team decides to leave the organization, especially now with virtual workforces. Steinway acknowledges the competitiveness of recruiting strong cybersecurity talent and being able to work remotely has increased competition in hiring.

Another challenge is budget, which almost all security leaders face. Steinway comments, "I have a very supportive executive team. They truly listen when we have needs and their trust is important to me. We've been very careful not to abuse that trust and we're always looking for ways to make us more efficient. We try to get the most out of our security technologies. We keep the toolbox as simple as possible, and especially pay close attention to the quality of the alerts and actions the tools are producing and make decisions accordingly. We try to be good corporate citizens from a spend perspective, but of course we do need to spend a little."

Visibility is also a challenge, especially with the diverse infrastructure at Audacy, Inc. Steinway says, "I have 47 individual markets each with multiple stations per market. Each station has its own engineering team. I must keep an eye on all of them. Visibility for me is key. I do not want to get caught by surprise in any way. That is where we've spent a lot of focus."

MEANINGFUL COMMUNICATION AND METRICS

Steinway approaches relationships with executives as mutually beneficial with strong alignment to demonstrate the value of security and gain buy-in across the organization. He meets with executives to understand their key initiatives and focus areas, then correlates security in a meaningful way to avoid being a hindrance.

He comments, "We are constantly looking for opportunities to say, hey, we have this capability already, or we have seen this in some other area. Between SecOps and DevOps, we are much closer to development activity and other changes that are taking place in the environment, and we will sometimes find opportunities to connect two business processes that may not have previously met. It is especially helpful to us to look for ways to simplify something, especially if it promotes collaboration and makes the business more efficient. That alone often reduces risk. We're not always focused on security doom and gloom."

To demonstrate progress to executives, Steinway leverages a standard set of KPIs that comprise a mix of the ISO and NIST frameworks. He makes sure they focus on showing progress around areas of improvement. These are also adaptable metrics, appropriate for a variety of executives or executive committees.

With regard to risk metrics, Steinway identifies action items or other items executives should be aware of, with a cohesive storytelling approach. After working in law and legal as a director of security, he learned that security metrics are not always about the technical details, but if you include a strong story that correlates to the other person's core objectives and goals, you gain their attention in a meaningful manner.

IDENTITY

For Steinway, Identity goes beyond accounts and systems. He explains, "It is also keys and certificates, it involves APIs as well as logins. It is not an individual credential, but also a system credential that should also be part of the identity program. In addition to general system access, we share data between systems, with partners, and all of that involves some type of authentication. So the identity program I'm trying to build would have some capability of detecting where credentials, of all types, are normally used and where or how they should not be used."

He continues, "It is more than just people and credentials. I would say there's two components. You must merge all of that credential data from disparate systems to create a picture. API keys, certificates, system accounts, right down to the number of dual-factor tokens that a user has registered. I want to get all that information into one place - like a business intelligence tool that can aggregate and enrich it similar to what organizations might do with customer data. Then I want to overlay some type of monitoring system on top of that so I can say these credentials are used in these places and that looks right, then baseline everything and look for anomalies. That's the perfect scenario that I'd like to build."