For the first 10 years of Dmitriy Sokolovskiy’s career he had first-hand experience with servers and datacenters, NOCs and SOCs, and consulted for defense contractors, public and private financial and medical companies, and non-profits.

Sokolovskiy then spent eleven years working at a security vendor, where he first built and managed the implementation arm of the professional services organization for Americas, personally participating in incident response and remediation for some of the largest breaches in US history. Later, he served as a Cloud Security Architect, helping protect the organization’s SaaS products utilizing CSA CCM and CIS CSC.

Currently, he is the CISO at Avid, a technology and multimedia company headquartered in Burlington, Massachusetts. Making the transition to Avid meant leaving an organization servicing a specific niche of the information security marketspace and moving to a holistic CISO role at a forward-thinking technology company. As CISO, he leads the build-out of the information security and privacy program, covering corporate and customer-facing cloud environments, and hardware and software products.

He explains, “The move to Avid was something I wanted to do, and I felt like I had a lot of experience both running a team in information security but also having seen all kinds of deployments and all kinds of issues over the years. I could combine those experiences together and apply it as a broad-spectrum application of security.”

BUILDING A PROGRAM FROM THE GROUND UP

When joining Avid, Sokolovskiy understood he was faced with a challenge as their first ever CISO, but it was a journey he was excited to embark on. The organization had no dedicated security function and Sokolovskiy was able to come in and implement a security program on his own terms as opposed to coming in and taking over an already established program.

This green field opportunity for Sokolovskiy was fully supported by senior leadership. To take on the somewhat overwhelming task of establishing a strategic, strong, and business-aligned security program, Sokolovskiy approached it by focusing on prioritizing and controlling his time.

He explains, “It’s important to control your resources. That will set you up for being able to do whatever you want to accomplish, if you do it correctly. It will also make sure you clear up any expectations that executive management might have about what you can accomplish. Everyone is on the same page that we’re not trying to build Rome in two days. I could work 120 hours a week and not cover all of the things that are coming in within that week. It’s important to be able to prioritize and to control your time really well and apply it to the most important things. I focused on continuously reviewing,
RISK AWARENESS AND DECISION MAKING

“Information security is never going to be about technical solutions. All the technology out there, it’s only a solution to one problem or several problems, but ultimately, it’s not going to achieve "security". It must come as part of this standardized and holistic decision-making approach. It has to be based on user and business awareness of the fact that every decision will have risks, and that the information security team is there to help them identify and measure those risks, and help figure out how to mitigate those risks in the most effective and cost effective way possible. And when they have that thinking and when reaching out to the security team for quick verification becomes second nature, then we can say that we’ve made the company secure. Every company’s going to get breached. It’s this risk awareness-based decision making process that’s going to allow you to survive with minimal impact, and keep the company, the employees and the customer information secure.”

FOCUSED ON INFORMATION SECURITY AWARENESS AND RISK DECISIONS

One of the top goals Sokolovskiy is currently focused on is information security awareness. He says his approach involves multiple angles including computer-based training similar to an online university for standardized mandatory training, as well as dedicated lunch and learn type activities and ad hoc agenda-less Q&A meetings.