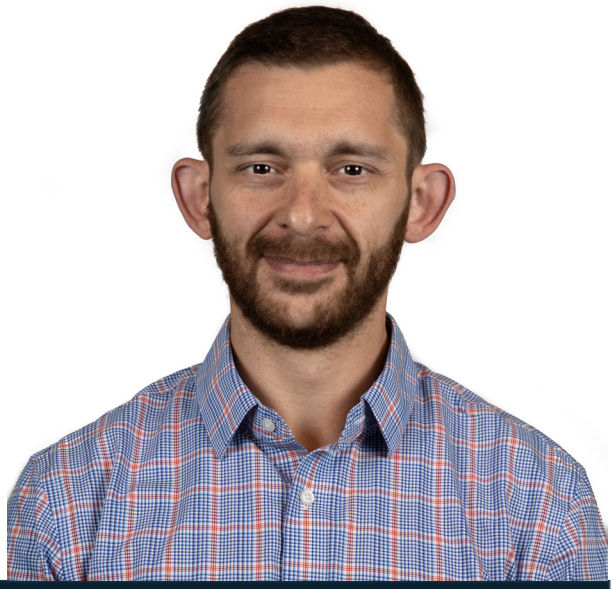
DMITRIY SOKOLOVSKIY

CISO, AVID



HEADQUARTERS: Burlington, MA

EMPLOYEES: 1,400+

REVENUE: $413 Million

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,

prioritizing, reprioritizing, then working without interruptions. As the team grew I made sure that they did the same, utilizing available resource management tools as needed. I've focused on managing resources well, concentrating on the important things, being clear about what we can't do, and continuing to provide good advice."

ASSESSING, STABILIZING, AND FORMALIZING THE SECURITY PROGRAM

It was vital for Sokolovskiy to make sure unplanned work, emergencies, and incidents did not derail his strategic plans and focus. Instead of reviewing and assessing the organization against a specific framework right at the beginning, he instead assessed against a live snapshot of issues they were actively facing, then worked on applying controls, process, redesign, or tools if necessary. Now a year and a half in, he says they are in a position where they can take a framework and apply and measure against it in a structured way without being continuously interrupted by incidents or attacks.

He says, "We chose the NIST CSF framework because it was distilled from several more expansive frameworks, yet made it much easier to follow and measure ourselves by. We're finalizing the formal self-assessment and gap analysis and we'll work on the structure remediation plan. But I can't stress this enough - that even before that's done, we had to "stabilize the patient", and only then use a more formal, structured approach to long term remediation."

FOCUSING ON 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.

He comments, "We are scheduling dedicated lunch and learns that are structured, goal-based lectures for employees, but we don't make them mandatory. Combined with that, we also have ad hoc agenda-less, but still structured, meetings. 'Lean coffee' is a style of meeting where employees come in and bring their topics and then everyone votes from the topics that were submitted. And we talk about them in order of voting. And sometimes we don't cover everything. We may leave some topics until the next time, but it's this continuous live information security Q&A that we make available to everyone in the company. Employees are getting access to trained information security personnel with experience, and we are getting continuous publicity with the employees to make sure they remember that information security exists. It's this continuously available source of information about security that becomes useful in their personal lives, which inevitably makes them more secure in their professional lives as well."

Another one of his top goals is changing the thinking around risk decisions. Their approach is not to have the information security team own risk decisions, but to be a guide to the business when they are making such decisions. Instead of the business coming to Sokolovskiy and asking if he approves a specific project, he is trying to institute a shift where business comes to information security to work together to identify risks and the risk level. Risks of different levels are then presented to management for written approval within the business unit, depending on the level of risk.

He explains, "Instead of being the blocker, we are a partner, and we are helping the business identify the risks on their level and then work with them to see if there's a mitigation control. But at the end, the decision and responsibility for that risk stays within the business. When it's owned by them, it becomes a very different process. Introducing this flow and changing the way business approaches risk decisions is probably the second biggest priority for this year."

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."