PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS WHO ARE LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

JOSH KOPLIK
CISO, IAC

HEADQUARTERS: New York City

EMPLOYEES: 5,800

ANNUAL REVENUE: $3.14 Billion

"In three years my role has evolved from program-building to enabling broader business objectives with security controls. Now business leaders are proactive in coming to me to discuss security as it relates to various strategic initiatives at the corporate level."

- JOSH KOPLIK

FIRST TIME CISO IN A NEW ROLE

When Josh Koplik joined the team at the media conglomerate IAC, he became the company's first CISO. It was also his first time in the role. He says, "It was exciting and refreshing to build the program from the ground up." Koplik says the chance to come into IAC as a trusted expert without inheriting any security "baggage" or pre-existing security programs drew him to the role.

IAC is a portfolio company, which Koplik describes as a "collection of loosely federated businesses." Each individual business, including well-known Internet brands such as About.com and Tinder, have their own IT team. The largest companies have dedicated security staff to handle the operational aspects of the IS program. Since the portfolio companies always had responsibility for security, IAC did not employ its own CISO until the Board of Directors made it a priority.

"To their credit, when a Board member inquired about information security at the company, the senior leadership recognized this area as a weakness and immediately sought to hire for the role. They made a very smart decision in that they aligned the CISO role outside of IT, giving me a lot of authority out of the gate," explains Koplik. "The senior team is very supportive. From the get-go, they have looked at me and said, 'you are the security guy, tell us what to do.'

Koplik reports into the Chief Administrative Officer, and regularly updates the CFO, General Counsel, and the head of Internal Audit on the security program. In regards to the finance and legal teams, Koplik says, "They want to know what is going on with security, so I am in constant contact with them. I do not

Security Challenges of Cloud-Based Businesses

Most of IAC's portfolio companies are only three to five years old. Nearly all of them are internet-based, consumer-focused brands. As a result, these businesses did not have to go through a Digital Transformation. Koplik explains, "These are companies that have been in the cloud from their inception. All the businesses are using Slack, all the teams are working remotely. If there is a trend out there, our businesses are on it. These are organizations that run at a rapid pace of change. That pace can bring about specific security challenges, so we need to be able to react quickly and keep on top of risks, even as new ones are presented all the time."

have to work for their attention."

SECURITY IS A BOARD-LEVEL PRIORITY AT IAC

Koplik presents a security update to the Board's Audit Committee every quarter. He says, "My reports are remarkably basic, and it works well that way. We are always measuring our progress against a scorecard. We have many businesses to track, and each one has its own set of risks. Each practice at each business gets a simple letter grade of A,B or C, to denote practice maturity."

The Board's interest and commitment to security empowers Koplik. He continues, "The Board wants to know of any problems, and 'problem children.' Thankfully, there are very few of those. The Board has made security a big priority, which makes it very easy to gain buy-in and acceptance of policy and programs at the business level."

ADVANCING FROM OPERATIONAL SECURITY TO STRATEGIC ADVISOR

Now three years into the role at IAC, Koplik is focused on governance, strategic direction setting and coalition building. While each business has autonomy to make their own security decision, Koplik makes recommendations, oversees risk assessments and leverages the scale of IAC's portfolio to negotiate better deals on security products that all the portfolio companies can leverage.

According to Koplik, "In three years my role has evolved from program-building to enabling broader business objectives with security controls. Now business leaders are proactive in coming to me to discuss security as it relates to various strategic initiatives at the corporate level. For example, as we look to opportunities in Europe, our executives want to make sure that they understand regional regulations and data privacy."

Koplik has two pieces of advice for CISOs that are working to establish security as a strategic business driver. He says, "First, do not overthink things. Until you get security operations figured out, there is no point in worrying about sophisticated measurement and key performance indicators. Stay focused on the things that really matter - the security hygiene of the business. A CISO has greater authority and more time to be strategic once their program is running well operationally."

He continues, "Second, do not be afraid to tell the truth. At IAC, the executives are very eager for reality. They want to know what needs to be improved. CISOs should not be scared to be loud about the important things that need to be addressed. You never want to disparage people, but you want to be honest. Of course, it is much easier to deliver this message from a position of credibility, and that is why it is so important to focus on getting the basics in place first."

STAYING FOCUSED ON SECURITY GOALS

Moving forward, Koplik and his team are focused on meeting two main security goals:

1. Improve Incident Response
He says, "We want to be much faster at detection. We want to be able to assess, contain and eliminate threats right when we find them."

2. Mature the Security Practices at Portfolio Companies
"My team is also focused on maturing the security practices at IAC businesses, including increasing staffing, and operationalizing security responsibilities such as vulnerability management within the businesses."

Koplik is putting programs in place to help IAC achieve these goals. "We are making a huge investment in security incident management right now," he says. "We are building and staffing a security operations center (SOC) at IAC to handle centralized incident response for all of the portfolio companies. This is a vote of confidence from our leadership and from our businesses that they trust Corporate to perform this function for them."