Corporate Security Teams Face a New Challenge Right In Their Backyards – Relevancy

Corporate security leaders discover innovative ways to remain relevant to the business, including new partnerships and pivoting to security as a service.

Corporate security teams face a new challenge in the threat landscape – relevancy to the bottom line.

Typically, board members view a security department as a cost center, and that's a perception security leaders want to change. Security department heads look for novel ways to illustrate how their department helps achieve the business's strategic goals. For example, the security executive for Take-Two Interactive Software explains his approach to proving his team's value.

When he first started his role at Take-Two Interactive Software, Joshua Levin-Soler, Senior Director of Global Security Intelligence and Operations, educated the company on what security means to the business.

"The company didn't have a real idea of what security was aside from a vague idea of what cybersecurity was," Levin-Soler said. "A lot of my role was educating our partners in what the potential could be and how we could assist them."

Levin-Soler shared that education goes both ways. Security experts should understand the comprehensive list of business initiatives instead of the one initiative that directly correlates to their job roles.

"One trap I think a lot of physical security people fall into is this notion that when you're looking at an organization, there's one set of objectives," he said. 'And that's a very dangerous view because when you're interacting with your individual stakeholders, their agendas may be dramatically different from the organization's objectives."

Kris Hamlin, Senior Vice President of Asset Protection Inventory Control and Logistics for Saks Off 5th, agrees that his biggest priority is remaining relevant to the business.

"My biggest focus as we move further into 2023 is keeping my team relevant and keeping us driving toward the strategic initiatives of the business, but doing it in an efficient and relevant way so that I can continue to grow my team," Hamlin said.

Chief security officers (CSO) look at the company's Form 10-K to align a business' goal with their own. Based on the form's information, CSOs can recommend proactive security initiatives to help stabilize the stock price, strengthen fiduciary responsibility, and increase stability in the supply chain. Additionally, the 10-K form lets the CSOs match individual stakeholders' agendas with the company's business goals.

Helping his team connect the dots, Kyle Klein, Head of Physical Security at Wealthsimple, trains his team on how to articulate the connection between security programs and business initiatives.

For example, Klein pushes his team to ask the following questions as they create security programs.

1. How can the security program connect back to driving profitability?
2. How does the initiative support or supplement strategic goals to drive profitability in the long run?
3. What are the risks to the organization if the program is not adopted?

"I coach my teams on how to build those plans and to take a look at the initiatives of the organization," Klein said.

Breaking down communications silos is another example of how corporate security teams try to remain relevant to a business.

Chief Executive Officer and founder of Center for Threatened Intelligence Janet Lawless advises her clients to create partnerships with other departments. "You need to collaborate in business. You need to be talking to all the teams because security and intelligence are not in silos," she said.

Security-as-a-Service (SECaaS) is a different approach corporate security professionals leverage to retain relevancy. SECaaS is a fresh concept that includes outsourcing security to a cloud-based vendor. However, security teams use the SECaaS model with internal stakeholders too.

For example, Klein from Weathsimple offers SECaaS to other departments within the company. "We recently helped the people operations team to identify and build out a high-risk exit strategy," Klein said. "It takes away that scary [thought] of, 'You're the security team. We don't want to talk to you,' which we get a lot of in the financial services [industry]."

Also, Klein shared that his previous company, an international e-commerce platform, discussed providing customers with SECaaS. "We started to approach the merchant side and see, 'Can we provide global event monitoring for some of our small merchants around the world?'" he said. "It doesn't drive revenue, but it creates a bit of a competitive advantage."
Protecting an organization's supply chain is another way corporate security teams influence a company's bottom line.

According to a study by the Association for Supply Chain Management (ASCM), supply chain risk and resilience, data security and cybersecurity, and logistics vulnerability are among the top 10 supply chain trends in 2023.

The ASCM report highlights, "Resilient supply chain design will also be critical to mitigating adverse events faster than the competition, providing excellent customer service, and generating value and market share."

Additionally, the report reveals that more supply chains are digital, increasing the likelihood of more vulnerabilities in their networks. Finally, the report discloses that companies should anticipate forging strong collaborations to safeguard networks, devices, people, and programs against bad actors –foreign and domestic.

Corporate security's involvement in defending a company's supply chain is crucial and elevates the team to a high-impact role. For example, Statista reports that in 2021 supply chain disruptions cost organizations globally an average of $184 million per year.

"You could measure [value] as that unit that protects the crown jewels of that organization or works with the crown jewels of that organization," Levin-Soler from Take Two Interactive said. "That's such an important point because if you can tie your work directly to preventing disruption, maintaining operations, and do that in a really compelling and crisp way, people are going to listen."

In the end, relevancy to a company's bottom line is how security groups can be relevant. Aligning team initiatives to an organization's business objectives is one step. SECaaS is another novel idea security leaders use as more of a competitive edge than a revenue driver. Defense of a business's supply chain and fostering internal partnerships prove successful in showing relevancy.

How is your team proving its relevancy to the business? Check out our resource library, and learn more about articulating your team's return on investment.