SEC

SECURITY EXECUTIVE COUNCIL

A research and advisory firm

Preparing Today's Security Leaders for the Threats of Tomorrow

Originally Published in Security Technology Executive Magazine

March 2014

Preparing today's security leaders for the threats of tomorrow

Former Starbucks security executive Francis D'Addario discusses the challenges facing contemporary CSOs

Earlier this month at the Great Conversation conference in Seattle, SIW had an opportunity to sit down with Francis D'Addario, the former vice president of partner and asset protection for Starbucks and an emeritus faculty member for the Security Executive Council (SEC). D'Addario leads the SEC's Next Generation Security Leader program, which is designed to provide security executives with the business skills necessary to survive in today's corporate landscape. For years, many businesses have seen the security department as a cost center rather than a contributor to the organization's bottom line, so it is crucial for today's security leaders to show how they're delivering value to the business.

What really brought this to the forefront, according to D'Addario, were the years following the 9/11 terror attacks when organizations put a lot of money and effort into security only to see no tangible return on their investment.

"Ten years ago, I would say that we were, ultimately, misaligned in terms of our assignment of being the all-hazard risk detectors and mitigators for major enterprises, corporations, NGOs and agencies," explained D'Addario. "Don't forget, after 9/11 we were on the job of being ever-vigilant, theoretically, and we spent trillions of dollars on security that did not have any viable payback in the decade that ran from 2001 through the (economic) downturn that we're just coming out of. What happened was there was a loss of credibility and a loss of confidence (in security)."

However, D'Addario said that in recent years, security practitioners have once again started focusing on enterprise risk management strategies that will pay dividends down the road and show the value proposition of security to the C-suite.

"I would say that in the last few years, we've put our eye on the horizon again. We are engaged in longer planning and that includes facilitation of a more effective supply chain for better risk mitigation outcomes for organizations, institutions and economies," said D'Addario. "Now we are assessing what the imperatives of management are and what the strategic goals of our organizations are. Our ability to measure our success is imperative. We can't have any more failures of confidence. We have to measure confidence and security and all of the risk mitigation processes that we bring to bear and we have to do that in a way that's viable for our stakeholders and our stakeholders' stakeholders."

Today's security leaders need to learn to align their departments with the imperatives and goals of the organization as a whole.

While it may seem like a simple exercise for security executives to learn to speak the language of business, D'Addario said that oftentimes one of the biggest hurdles for CSOs is just learning to stop and listen.

"When you listen, you're going to find the leadership imperatives of your organization very well enunciated," said D'Addario. "For our senses, particularly in the communications realm, we have people that are going to be audio learners, we're going to have people that are going to be visual learners that have to see the charts and graphs, and we have people that have to read it. I think we have to take a multimedia effort in not only listening, but anticipating that when we're reviewing the text or we're reviewing the symbolic iconography of whatever the value system or strategic objectives are of the organization, that we're not only in full alignment with all of it but we're enabling it, we're having a discussion around what are the risk implications to those lofty imperatives and goals and we're mitigating against those all of the time."

D'Addario believes that one of the biggest challenges facing today's security executives is the shear velocity of change in global connectivity.

"We talk about how technology brings the deck of distance, it really also compacts your ability to analyze and use intelligence in a way that's beneficial," added D'Addario. "We

now, through the World Economic Forum and others, have a really good understanding of what risks are and what the economic consequences of risk are. We understand that a food crisis in another part of the world can affect the general stability of governments; we understand that the fiscal crisis of collapse can crack the economics of nation states and regions; and, we understand that socio-political changes up to and including war, revolution and terrorism are things that we have to deal with and have very real world consequences for the supply chain and confidence on the movement of goods and information."

Additionally, D'Addario believes that security practitioners need to be good students of the successes and failures of their colleagues in these aforementioned threat environments.

"How are other people dealing with it? What is the consequence of their intervention, their timing, their people, processes and technology applications?" he asked. "At the end of the day, what's the bottom line for the organization? Is it confidence? Is it financial gain? Is it the capability of stewarding finite resources in an NGO and being able to inoculate everybody in the world?"

While the capabilities of security technology such as video surveillance and access control have grown by leaps and bounds and everyone recognizes the benefits of a truly integrated system, D'Addario said that security leaders sometimes have a tendency to take their "risk hat" off when they're looking for the perfect solution to address their needs and forget about the potential liabilities.

We're not asking ourselves, 'what are the risks to my network of this particular peripheral?' In the old days, the chief information security officers and chief technology officers would say everything is buttoned down, but nothing was integrated so it was a hassle for the consumer to use," D'Addario said. "As you're developing integration, you've got these sorts of opportunities to be able to disadvantage the network, be able to pick up protected data off of those networks, etc. Having smart devices that really give us the analytic capability of true access control, just-in-time needed analytics and management information to run and enable a business, we have to make sure that those features are not opportunistically available to people that would wish to harm us or rip us off."

The recent data breach at retail giant Target has also raised awareness among CSOs about the need to balance protecting traditional physical assets with securing information that organizations now collect in cyberspace. According to D'Addario, the key to striking the right balance is "narrowing to the critical few."

"If you know you have supply chain in 31 countries, but the supply chain is disparately under five percent in 30 of those counties and 17 percent from one country, spend your time on your biggest supply chain arena," he said.

Francis D'Addario is an emeritus faculty member of the Security Executive Council and a former security executive at Starbucks.

About the Security Executive Council

The SEC is the leading research and advisory firm focused on corporate security risk mitigation solutions. Having worked with hundreds of companies and organizations we have witnessed the proven practices that produce the most positive transformation. Our subject matter experts have deep expertise in all aspects of security risk mitigation strategy; they collaborate with security leaders to transform security programs into more capable and valued centers of excellence. Watch our 3-minute video to learn more.

Contact us at: contact@secleader.com
Learn more about the SEC here: https://www.securityexecutivecouncil.com