SEC
SECURITY EXECUTIVE COUNCIL
A research and advisory firm

What Will Security Look Like in 2020?

Francis D’Addario, Bob Hayes and
Kathleen Kotwica, Ph.D.

Originally Published in Security Technology Executive

Updated December 2016

What Will Security Look Like in 2020?

Created by Francis D'Addario, former vice president of Partner and Asset Protection for Starbucks Coffee and emeritus faculty member of the Security Executive Council; Bob Hayes, former CSO of Georgia-Pacific and managing director of the Security Executive Council; and Kathleen Kotwica, PhD, executive vice president and chief knowledge strategist of the Security Executive Council

By the year 2020, what should "security" look like? Organizations are now more complex than ever before and there's no evidence that the trend will reverse. There are five important elements a security leader should aim to incorpo-rate into his or her security program if it is to approach a level of effectiveness and efficiency. Companies have adapted to succeed in a global and decentralized market economy, increasing reliance on vendors, suppliers, and contract staff for what were previously in-house operations. They have changed their internal structure to better compete in changing markets and a down economy, and they have learned to leverage new technologies to increase the speed of both communication and business.

This complexity has brought new risks that pose an ongoing security challenge, at a time when security is already arguably at a disadvantage. Many institutions still have not regained confidence following the decade of security shortfalls that began in 2001. Global markets and governments face continued uncertainty, leading many businesses to stop investing in new infrastructure and programs and to instead cut costs and staff in an effort to weather a storm that may or may not be coming. Yet if organizations do not develop or maintain a robust risk strategy, they could suffer stunted growth and loss of revenue.

How should security evolve to excel in this environment?

Some organizations have accepted the challenge to push security toward value enhancement and stronger, more consistent protection through the rest of this decade. They're already giving the industry a glimpse of what security could—and, perhaps, should—look like in the next decade.

What Security 2020 Could Be: A Case Study

The CSO begins the day briefing the rest of the C-suite on mitigation opportunities that the company's unified risk oversight team is tracking. He helped provide the momentum to convene the first risk council that over the years has morphed into a diverse, cross-functional collaboration; gathering crucial and timely insights from across the company to both identify and address hazards earlier and better than previous siloed efforts.

The CSO is a business partner who is actively engaged in responding to key operational needs. His team pro-actively seeks alignment with the business' goals through regularly scheduled meetings with business unit leaders.

Once relied upon for heroic efforts to protect personnel and assets, the security function's strategies have evolved to incorporate relevant performance metrics, including compliance certainty and contribution to plan. Security owns or plays a pivotal role in a wide range of organizational priorities, such as sales and supply chain exception reporting. Conventional fraud detection and response are augmented with cost avoidance planning, brand reputation protection, and corporate social responsibility, including community disaster preparedness. Security consistently applies its unique perspective to help build process and value improvements into these other functions.

The function is also advancing integration capabilities for the entire organization and the industry by participating in technology test beds. Partnering with solution providers, selected locations model, test and prove the effectiveness of integrated security technology elements. Data is shared with operators and vendor and integrator partners to influence product and process improvement. In some cases, security is using technology manufactured by its own company to influence both risk mitigation and revenue.

Collaboration is a hallmark of the unified risk mitigation security strategy. Security maintains multiple internal and external information-sharing partnerships with public and private organizations, and it also works to forge a strong link with the community through social responsibility and philanthropic efforts.

The CSO's voice is requested and heard by other senior leaders and the Board because of his experience and focus on business integrity and value; but his function does not falter in his absence. Superior performance, excellent insight into risks on the horizon, and refusal to exploit fear, uncertainty and doubt have restored the confidence of management and other stakeholders. Security focuses on mentorship of inter-generational talent and leadership development to ensure that the function's opportunity to influence is not lost when the CSO cannot make the call. Determined leadership and the evolution of the security function have resulted in contributions to the bottom line, a strong organizational emphasis on the value of security, higher stakeholder engagement, and measurable improvements in negative security events and business resilience.

While the example of the CSO at the beginning of this section is not company-specific, it is not hypothetical. Each of the elements that contribute to success in our illustration is in place today at one of several organizations with which we have worked.

Elements of 2020 Security

There are five important elements a security leader should aim to incorporate into his or her program if it is to approach the level of effectiveness and efficiency of the case study in the previous section.

1. A focus on board-level risk

We've identified nine categories of risk that are commonly of interest to boards: financial, business continuity and resiliency, reputation and ethics, human capital, information, legal, regulation/compliance and liability, new and emerging markets for business, and physical/premises and product. Your board's concerns may differ from these, but this is a good place to start.

Get to know and understand what risks your board is most concerned about to determine which ones have security components. Determine whether you can line up your existing security programs with one or more of those concerns. Once you've categorized your existing programs, look at the categories in which security has little or no impact and think about what you can do to provide value in those areas. Update your strategy to focus on programs that deal with these risks, and then communicate your work clearly to senior management.

2. **Unified Risk Oversight™**

Security does not "own" unwanted risks. Resilient organizations understand this and set up cross functional groups to share information and oversight on risk issues. There should be many groups involved in risk oversight, including business conduct and ethics, compliance, legal, privacy, audit, and security (see Figure 1). Each of them owns or monitors some function that can provide detection or prevention of risk.

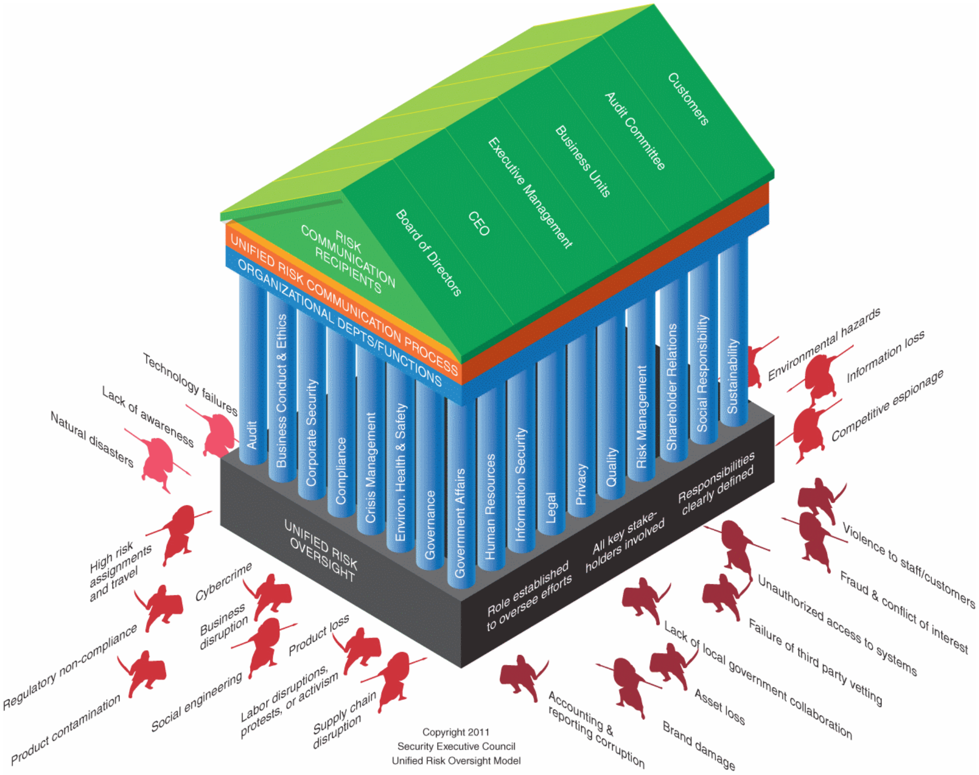

Figure 1. Unified Risk Oversight™ model

3. All-hazards risk mitigation

Recognize that risk to the organization comes in myriad forms, many of which are not traditionally owned by corporate security functions. Risk mitigation need not confine itself to traditional corporate security risks; in fact, in many organizations, “risk” has been removed from corporate security’s purview because of their traditionally narrow view. Risk must be viewed at an organizational level—high ground from which one can see and anticipate hazards of all types.

4. Innovative integration

Programs exist that connect integrators, technology/service providers, and security practitioners for the purpose of testing and proving cutting-edge integrated solutions to provide a total security format with proven return on investment. This requires providers to focus on the needs of the 2020 organization rather than on product sales; organizations to open up the kimono and share metrics of product success; and integrators to step out of the comfort zone of a single product line and begin to think more creatively about integration options that could add value for their customers. If these three stakeholder groups in our industry collaborate in testing for improved interoperability, all will benefit.

5. Inter-generational training

Our research shows there is a wide gap in the transfer of valuable knowledge to new and advancing security leaders. This means the next generation of security leaders is finding that in many respects they must begin anew when their predecessors retire or leave the organization, rather than building upon what their predecessors accomplished. Without training and mentoring in place, the security program will eventually take two steps back for every two steps forward.

Are you and your organization evolving toward the Security 2020 ideal? We would like to hear from you. The Security Executive Council has been building solutions and working with its approved Solution Innovation Partners to make Security 2020 a reality. Watch for updates by signing up for our news- letters, join our working groups and LinkedIn group to contribute, or become one of the Tier 1 Security Leaders driving the change. To share your stories or to find out more, drop us a line at contact@secleader.com.

About the Security Executive Council

We are a research and advisory firm for security leaders. We have a collective of close to 100 security subject matter experts that have been successful security executives or are recognized industry experts in their field. The resources and tools we develop are constantly evolving to provide maximum value. Some engage with us by way of multi-year "retained" services agreements (Tier 1 Stakeholders). Tier 1 Stakeholders are those that want support on an ongoing basis but also want to have an active role in identifying solutions for the industry. Others come to us seeking a specific solution to a contained issue. In all the ways people engage with the SEC the bottom line goal is to help define and communicate the value of the Security organization.

Contact us at: contact@secleader.com

Learn more about the SEC here: https://www.securityexecutivecouncil.com