SEC
SECURITY EXECUTIVE COUNCIL
A research and advisory firm

Security Program Strategy & Operations > Emerging Issues >

Forces of Change: What's on Senior Management's Radar and the Potential Impact on Your Security Strategy

By the Security Executive Council Faculty & Staff

Security must continually evolve their mitigation plans with emerging risks; keeping up with change serves to impact security's role, methodologies, and value in the organization. The Security Executive Council's (SEC) Security Leadership Research Institute has been following trends that should impact security strategy decisions since 2007. By recognizing the trends that senior leadership is watching, risk mitigation professionals can be better prepared to have discussions around how security programs can contribute to the reduction of unwanted risk. Following is a brief report of current trends.

What Executive Management is Reading

Forbes, The Wall Street Journal, Bloomberg Businessweek - publications like these help direct the attention of CEOs worldwide toward issues that may impact their companies. Security issues are increasingly occupying their pages.

When your boss emails you an article and asks, "What do you know about this?" you'll want to be prepared to discuss it. We've tracked a few trends of executive interest that are likely to come up in board meetings and hallway conversations. If you're not ready to talk about your response to these issues, now is a good time to examine them.

Persistent Background Screening

In June, the Department of Defense announced that it would incorporate continuous screening into its background investigation program for new defense employees, a responsibility newly transferred from the Office of Personnel Management. The goal is to decrease the government's massive screening backlog for new hires, but it's also a response to reports that the Navy Yard shooting of 2013 may have been prevented if mental health and arrest records of the shooter, a contractor with security clearance, had been reviewed after hiring.

Persistent background screening, sometimes called continuous or rolling screening, requires employers to provide employees' personal information to a service provider that then continually monitors public records to inform the employer of changes in criminal history, legal actions, licensing, or financial records - changes that could increase the employee's chances of becoming a threat or a liability to the organization.

In theory, this type of screening would help organizations intervene in advance of potential workplace violence and insider threats. The legal picture is unclear, however, and concerns about inappropriate termination, reporting errors, and consent to screening may take a while to be settled. Be aware of the pros and cons of this type of screening so you can knowledgably inform your executives of its implications for your organization

Integrating Physical and Cyber Security

While this topic has been covered extensively in security publications over the last 10 years, it's only recently begun to buzz in business media. To some extent we have the Internet of Things to blame for that. After all, when devices of all types now include a networked or data-sharing component, major retailers can get breached through their air handling systems and casinos hacked through digital fish tanks. These events have reliably and frequently made the headlines, and senior business leaders have noticed.

Recognizing that many threats have both physical and cyber components, many companies have already shifted reporting lines to ensure that the cyber and physical security functions work more closely together. Some merge the functions entirely, while others institute parallel reporting to a common executive.

Be thinking now about where your function fits in your company. Which structures would work to help security respond to integrated threats, and which wouldn't? What communication challenges might you face? How might such changes impact your services and resources?

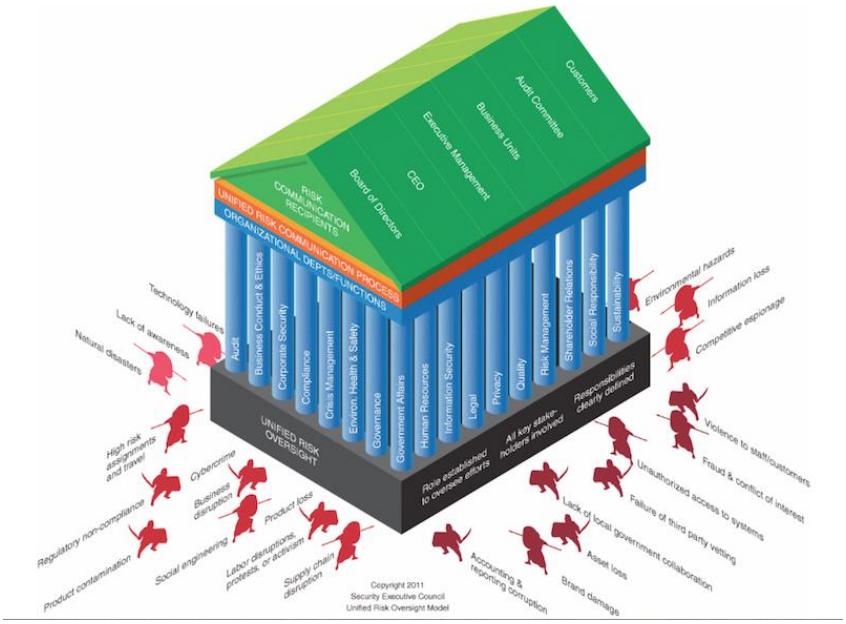
Fusion Centers

Another facet of physical and cyber security integration trending with executives is the idea of a fusion center, based on public sector emergency response models, which combines the different aspects of security across the enterprise. When executives realize that threats are multifaceted, it becomes clear that response to events must be integrated and interdisciplinary. Both small and large companies have begun moving to the combined fusion center crisis response model. What impact would it have on your organization if you are asked to shift to an integrated fusion center model?

Operational Risk and Business Alignment

Generally, when companies assess their risk for their yearly 10K reports, the top 15 or so risks identified are assigned to top executives and tracked. But what about the other 200 items on the list? Many of these fall into the category of operational rather than enterprise risks - risks that result from inadequate or failed internal processes, people, and systems, or from external events. These risks have the potential to cause significant damage. Take, for example, United Airlines' much-publicized mishandling last year of a passenger who refused to deplane - an operational issue that reportedly cost the company millions in brand damage.

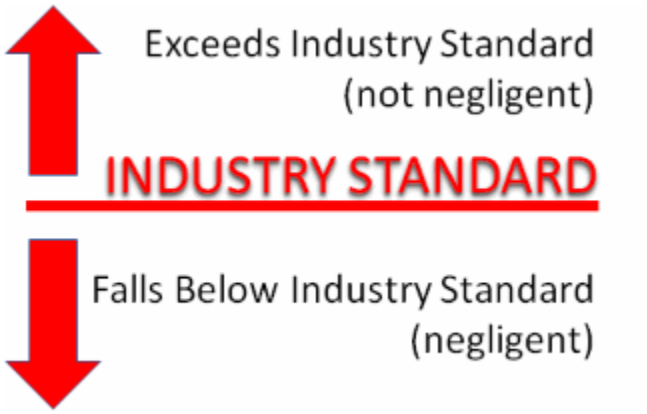
One challenge in dealing with operational risk is that when it's taken into account, every function in the organization becomes a part of the risk mitigation picture, but there is seldom a structure that unifies all these parties to manage that risk.



The SEC's Board-Level Risk (BLR) and Unified Risk Oversight (URO) models are two popular structures for managing enterprise security risks.

We have talked extensively with many clients about convening Operational Risk Leadership Advisory Councils as well. These ORLACs allow those on the operational side of risk management to advise an organization on issues that otherwise may be outside its field of view. Recently one of our clients consulted successfully with their ORLAC to decide how to manage on an operational level the shift to an open carry campus. Learn more about how BLR, URO and ORLAC can enhance Security's role as a team player in ERM efforts.

Security Program Defensibility



High-profile mass shootings and workplace violence incidents have executives thinking about legal liability for harm inflicted on their property. Negligent security is an arm of premises liability under which landowners can be sued if injuries occur on site. In short, companies can be sued for having inadequate security programs.

Plaintiffs use "professional security standards" to set the bar for adequate security, but many of these physical security standards are vague and poorly developed - presented more as considerations than actual requirements.

In one such case, a third party came onto the property and shot multiple people. The company, sued for negligent security program, had to produce millions of pages of documents to support their security program's diligence and validity.

Don't be surprised if senior leaders come to you to ask you how you will defend your program if a similar event were to occur at one of your sites. (For more on this, check out the summary of the SEC's State of the Industry presentation on program defensibility)

Additional Trends Within Security

In addition to these executive concerns, we've researched issues that are trending with leaders inside the security function. Here are the top five, to be covered in more depth in a future article:

- Risk-based or standards-based security, is one more influential than another?
- Revisiting core security programs for new options and optimization.
- Increasing executive awareness, concern and expectations of security capabilities and roles.
- Managing the fundamentals of comprehensive risk assessments.
- Enhancing executive influence by offering research-based, methodologies and strategies.

Visit the Security Executive Council web site to view more resources in the Security Program Strategy & Operations : Emerging Issues series.

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
Website: https://www.securityexecutivecouncil.com/

