SEC
SECURITY EXECUTIVE COUNCIL
A research and advisory firm

Wanted: A New Type of Security Leader

Bob Hayes, Kathleen Kotwica and Francis D'Addario

Originally Published in SecurityInfoWatch.com

April 2013

Wanted: New Type of Security Leader

As the recognition of board-level risk continues to grow across the enterprise, so too does the need for highly trained business executives with security expertise. Today's all-hazards corporate risk environment will tolerate nothing less than security executives that are as smart, prepared, vigilant, and progressive as the ever-present risk they will attempt to mitigate.

Security executives must be versed in enterprise risk mitigation and ensure that their perceived organizational risks outlined in their 10K statements are aligned with a unified risk mitigation program. So many parts of a business are impacted by these modern requirements, corporate security is no longer purely a threat detection and mitigation problem, but a systemic, corporate culture issue that needs to be implemented, staffed, and managed accordingly.

But is the industry doing all it can to ensure we're creating business people that know security? An honest assessment reveals that while the industry has done a lot to prepare "the boots on the ground" to manage and mitigate the security risks for the individual lines of business, the convergence and elevation of corporate security to board-level risk has created the need for a new type of security business executive, at the same time creating a gap in the information and resources available to properly train and prepare this new breed of business executives in the complexities of business-based corporate security.

How Corporate Security Executives Have Evolved

The evolution of corporate security to its place as a board level consideration has had a somewhat segmented and utilitarian trajectory over the past 60 years, with each decade being marked by an emphasis on a different aspect or approach.

- **1960s**: The security industry’s nascent period in the years following WWII through the 1960s was heavily defined by the influx of GI’s returning from overseas. These ranks proved a plentiful and capable workforce for prevention, detection, and response.
- **1970s**: The security industry in the 1970’s was heavily influenced by the cultural shifts that were taking place in the country. Societal problems were being hired into organizations, which created a need for more internal investigations and prosecution.
- **80s and 90s**: By the late 80s and early 90’s organizations became very interested in corporate culture and were eager to appear on lists of the numerous *100 Best Places...* lists that were coming into vogue. Organizations began vying for the best security talent to bring into a company and were no longer interested in simply hiring “police officers” to run their security programs. Senior management began looking for professionals that embodied and could promote the corporate culture.
- **90s and 2000s**: By the late 90's and 2000's, technology started to become integrated and integral to all parts of the business, and the security focus began to shift to things like network penetration, application security, and platform security.

As the security industry passed through each phase, senior management looked at security in a singular manner, often defined by the most recent security situation they had to deal with. If an organization had a loss of life on an international business trip, it became the focus.

As the internal security focus would shift based on one of these incidents, senior management felt they must go outside the organization to acquire talent with this new required skill set, instead of realizing they had it internally. As a consequence, security professionals also began to view their profession through silos, and as one set of requirements gave way to another set, security professionals found themselves defending their skill set, as opposed to going out and acquiring new ones.

- **Today:** This chronological shift in the profile of corporate security and the required skill set of security practitioners coincides with an exponential increase in the sophistication of doing business in a modern global economy, which has resulted in senior management looking at corporate risk in a more sophisticated way now. That sophistication demands the ability to understand and respond to very specific (often divergent) types of threat, while at the same time being able to develop, implement, and manage unified risk programs that are seamless across all business units and consistent with organizational culture.

Security practitioners that happen to have business-side experience will find themselves better prepared to thrive in this demanding environment, and those that do not possess a business background will need to bridge the gap in the following several core areas if they hope to be successful.

Dealing with Upper Management

Security has really never been viewed or taught from the P-side of a P&L. It's critical that security leaders not only understand what the organization's security needs are, but also be able to articulate the value of these security services and programs to an organization's bottom line, or prove that their programs are cost neutral. Developing this set of specialized information, resources, and expertise is an imperative that has the potential to be game changing.

For security and business to be a truly unified discipline, there needs to be a common and shared language for defining risk and mitigation, and articulating the success (or failure) points for any given initiative. This common language needs to be accessible and inclusive to all units with an organization, including executives, HR, Legal, Finance, Security.

Additionally, today's security executive needs to be committed to communicating their plans as part of SEC 10K statements and then actively work to achieve that alignment. Private companies that don't need to file 10K statements should also be committed to communicating their perceived risk to their board and implement a unified mitigation strategy. This requirement has all parts of the business ramping up their security efforts. The message here, is if you're a security executive who's approached senior management in the past (perhaps unsuccessfully) about a unified approach to enterprise risk management, go back and try again; they're more likely to listen at this point.

Matching security with Company Culture

Today's security leaders need to attend to their organization's "state of readiness" for their proposed programs. That is, does senior management view security the same way as the security practitioner? If not, there will likely be misunderstandings that prevent the most successful partnership involving security programs. As well, corporate culture needs to be attuned to. The Council has done research in this area and has found different categories of corporate cultures that will have an impact on how programs need to be built and communicated. For example:

- All about the people
- Analytical and logical
- Utilitarian and focused on getting the work done
- Reserved/guarded
- Innovative
- Parental in nature

New Blood and Heightened Awareness

With the first group of baby-boomers reaching retirement age in 2011, we stand next defining chapter for our industry. While the workforce will contract, the risks to be mitigated will continue to escalate. And with escalation, brings awareness, which is evident by the fact that the business trade magazine are writing about it, the events around it, and laws passed about it. However, while there is much coverage of risk in business, it's usually from the views of specific business functions; no one is talks about how we are going to all play together to make this unified vision of risk management happen.

This heightened state of awareness and attention to board-level risk can certainly lead to positive things, assuming the right people are in place leading the effort. We as industry practitioners must take an active part in providing current and emerging business leaders with tested and validated security knowledge best practices presented in a business management context. We must also seek to partner with other entities and industries, including higher education to develop highly specialized, comprehensive, security/business curriculum.

Six Best Practices of Today's Security Leader

Our research shows the most successful practices are rooted in risk theory and business processes, focused on application and value contribution, to arm security managers and other risk mitigation managers with the business leadership acumen necessary to propel them and their organizations to the next level of strategic performance. These best practices fall into six core areas:

1. *Aligning board-level risk and mitigation strategies*

Managing brand reputation requires cross-functional risk mitigation oversight for people, assets and critical processes, including board-level risk and unified protection business-unit considerations for relevant assessment and mitigation strategies.

2. *Communicating all-hazards risk, mitigation, and performance metrics*

Boards, management teams, and stakeholders increasingly make critical decisions based on a host of divergent data, spreadsheets, graphs and analysis. Effective, actionable risk management requires discipline. Understanding data to identify risks and tell a compelling story of injury, loss, damage and cost avoidance is our objective.

3. *Run security as a business*

Practitioners must remember they are "selling" their services and programs: you need to know the marketplace, your customers, program capacity and value. Our research shows there is no one common type or even universal “best” security model – you have to do the business research to make the best decisions.

4. *Influencing community all-hazard preparedness and resilience*

Catastrophic, man-made and natural risks continue to threaten organizations and communities. Incident, crisis and continuity management are increasingly important. Practitioners need to be aware of the latest global requirements for preparedness compliance; as well as the means to protect brand with alliances.

5. *Adding incremental value with mission assurance and P&L performance*

Board-level risk mitigation is no longer just consequence protection. Business acumen quantitatively and qualitatively enables a path to value. Practitioners should be versed on connecting revenue influencing and cost avoidance for return-on-investment and operating results.

6. *Managing information protection, breaches and situational intelligence*

Brand stakeholders require confidence. Information ranging from intellectual property assets to personal identifiers must be protected from persistent physical and cyber threats. Practitioners need to road-map protection architecture and manage information crises.

Additional areas the Council has identified through its research include: Managing extreme risks; evolving operational excellence; assessing next generation executive(s) and service organization(s); achieving all-hazard preparedness for resilience; compounding value beyond mission; and managing uncertainty for confidence.

Embracing and building corporate security programs around these core areas is not only critical for security executives working today, but also to the emerging leaders of tomorrow. Providing this type of security business education to tomorrow's leaders before they hit the workforce has huge implications for our industry's ability to continue to respond and remain current with corporate risk.

And it will be up to the next generation of security leaders to seize upon the opportunities facing them, the industry, and the organizations they work for. Unified risk oversight is no longer only a practitioner concern or a senior management concern, it's an enterprise-wide concern impacting all levels and units within an organization. There's no longer a single point of failure – there are lots of players and moving parts.

Who will lead the effort? The answer is it will take a new type of security leader.

Bob Hayes is Managing Director, Security Executive Council (SEC); Kathleen Kotwica, PhD, is EVP and Chief Knowledge Strategist; Francis D'Addario is the former CSO of Starbucks Coffee and Emeritus Faculty. The SEC (www.securityexecutivecouncil.com) is a problem-solving research and services organization focused on helping businesses build value while improving their ability to effectively manage and mitigate risk.

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