Managing Enterprise-Wide Board Risk

Created by Dick Lefler, Kathleen Kotwica, Ph.D. and Bob Hayes, Security Executive Council faculty and staff

- Increasingly, regulations make board members accountable
- Each function of the organization has board level risks to address
- Is each element of the business doing its part?
- A process to ensure Unified Risk Oversight™ is needed

Sometimes great ideas come with big consequences. The continued business trends toward globalization, advantages of economic scale, and strategic partnering are multiplying corporations' opportunities, but they're also acting to multiply the impact of risk failure. One risk failure at a single point in a company or its supplier network - particularly one picked up by the media - can now have a profound effect across the entire enterprise, placing a company in jeopardy far beyond traditional measurements. It is clear, for example, that the failure to properly design a gas pedal can create repercussions beyond the scope and imagination of an automobile company's engineering department.

Risks occur in all size and shapes; most can be and are responded to correctly, but the failure to recognize the potential consequences of a risk failure beyond the initial report can bring serious damage to companies. Add to that the scandal-induced requirements for greater accountability and oversight, and it's clear why we've seen an increased push from the board of directors and senior management to conduct enterprise risk assessments and follow through with robust risk management.

Traditionally, risk management has been coordinated by only a few business units of an organization. This may make sense for some industries, but for most, an approach coordinated across the enterprise will yield better risk mitigation strategies and tactics.

A Conceptual Risk Picture

As management and the board strive to develop a clearer picture of risk in their organizations, they should endeavor to look across all functional groups to review, organize and monitor the company's diverse collection of risks. The Security Executive Council, a problem-solving research and services organization that involves a wide range of risk mitigation leaders, has analyzed many corporate enterprise risk assessment plans and strategies to identify common concerns and opportunities to create a more consistent risk oversight process. The work was part of a research initiative to create a baseline corporate risk landscape that shows security's involvement in risk management.
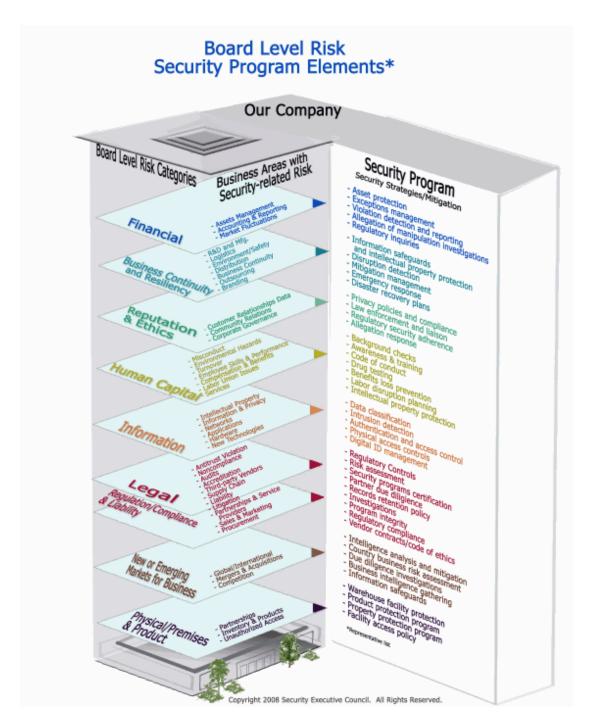
The focus of the study was to identify risks that had security-related consequences and areas in which security mitigation strategies would add value to overall enterprise risk reduction. However, this process of risk identification and classification could be applicable to any function of the company.

After analyzing numerous and diverse enterprise risk assessments, the Council identified common risks that faced corporations. These were organized into eight descriptive categories (left column of following graphic).

Next, they identified activities under each category that had related security risks (second column). This list represents many of the risks the Council community has typically encountered, but is not meant to be an exhaustive list.

Last, the Council drew upon the successful practices and experience of its large faculty of former security and risk professionals (its Collective Knowledge™) to match security mitigation strategies to each "floor" of the corporation (third column).

The purpose of the research output was to provide a direct link between the business category and the potential use of a security program to mitigate the risks identified. Why security? Most security programs are designed to cross all business units; that puts the security function in a strategic position to help provide enterprise-wide protection against an array of risks. Security protection programs do not by their nature have to belong to the corporate security department. Instead, they are often shared programs in which a team comprising several business units collaborates to provide risks mitigation. Coordination with human resources for new employee background verification process is a classic example, usually employing HR, security and legal.

[Figure 1: The graphic depiction of the Security Executive Council's research: enterprise risks, business activities with security issues, and security programs/mitigation strategies.]

Council Tier 1 Leaders use this tool to map how the security function can add value through risk mitigation strategies across the enterprise. They report that displaying the risks in line with the values of the board helps them gain support and move initiatives through the organization.

Security's Role in Risk Management

Many companies have found that some proactive security programs must be considered during, and integrated into, planning for new product and business program introduction. However, risk losses are too often considered to be onetime variable expenses for which planning cannot be justified. The opposite is true. Such events as fraud and criminal attacks are normal in the global marketplace. Determining the extent of those risks, examining the cost of mitigation, and including that cost as part of the fixed cost is necessary for product launch.

A global supply chain study conducted by Stanford University demonstrated that the security program's inclusion in the basic movement of goods in the supply chain not only reduced shrinkage but enhanced productivity, lowered costs and increased the speed of shipments involved in the study. Imagine a security program enhancing operating margin, speeding delivery, and enhancing customer relationships while also mitigating risks.

Enterprise Risk Council

To enhance their focus on the risks confronting their organizations, more companies are moving to establish enterprise risk councils (ERC) composed of key business leaders who offer broader perspectives on the various risk concerns. This ERC format is designed to provide the same holistic approach to risk mitigation that the board provides for identifying and understanding risk.

The ERC carries out its duties by allocating resources, analyzing cost benefits of mitigation solutions, and providing report card information to senior management for review with the board of directors. In this model, audit reviews and analyzes the ERC's success in accomplishing its duties. The audit committee reports are used in part to determine executive compensation in connection with risk management and mitigation. The simple absence of a risk event does not guarantee bonus compensation, but the board's compensation decision should be driven by management's attention to identifying and managing risks.

Next Steps

It is critical that all functions play a role in understanding the new risk landscape. The corporate secretary has the opportunity and possibly the obligation to promote and govern board-level risk analysis. The research and conceptual graphic provided here was intended for security leaders, but this same process could be used with all staff groups and revisited regularly within the company. Having a common "picture" to help create a risk-aware enterprise and a model of Unified Risk Oversight™ can be a useful exercise.

Visit the Security Executive Council website for other resources in the [Risk-Based Security: Board Level Risk/ERM](#) 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 here: https://www.securityexecutivecouncil.com/