SEC
SECURITY EXECUTIVE COUNCIL
A research and advisory firm

Risk-Based Security > Board Level Risk/ERM >

Balancing Board-Level Risk

Created by Marleah Blades, Security Executive Council Senior Editor

The risk management failures of the financial community have left their mark on businesses of all types, through both the global economic crisis they ushered in and the resulting scrutiny of corporate risk oversight. The oversight role of the board of directors has been the target of proposed and implemented reforms including the Security and Exchange Commission's enhanced proxy disclosure rules and the Dodd-Frank Wall Street Reform and Consumer Protection Act.

Board directors have commonly been held responsible for the risks that impact their organizations, but the increased transparency of these requirements helps raise their profile and creates a greater potential for personal accountability in case of failure. While some boards are focusing on risk oversight more earnestly than others, many are re-examining their structure and processes to ensure that risk is appropriately identified, managed, and monitored. The security function will continue to feel the impacts of these changes as boards of directors work to adjust to requirements and broadened expectations.

The Oversight-Management Cycle

Risk oversight is sometimes confused with risk management; however, the two are complementary but separate functions.

Risk oversight entails "setting the tone at the top"—specifying the culture of the company, identifying and prioritizing the risks the company faces, defining its risk appetite, and monitoring management's handling of risk to ensure it is in step with that appetite and culture.

Risk management, on the other hand, is the implementation of policies and procedures to transfer or mitigate the identified risks that cannot be accepted by the organization. Risk oversight directs risk management, and both either directly or indirectly influence the security function.

The full board is responsible for risk oversight, but portions of it are generally handled by board audit or risk committees, which are increasingly being assisted by outside parties, says Dick Lefler, former vice president and CSO of American Express and current Chairman and Dean of Emeritus Faculty for the Security Executive Council.

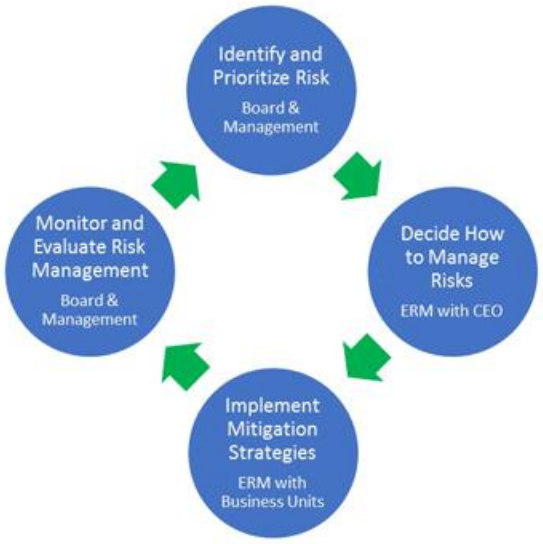
"In the last two or three years, we have begun to see more consulting services specifically engaged by large global companies to come in and systematically identify risk in all the different parts of the enterprise, then group and prioritize those risks," he says. "Clearly, companies are increasingly embracing an enterprise risk management approach using distinct business and staff units to collectively work together and manage risk. The use of consultants to capture and identify risk is a complementary skill set that a lot of ERM teams are using to help them get an enterprise picture and understanding of the risk.

"It also provides an independent perspective for the board to understand what the risks are so that they can influence the CEO and the senior management team to provide resources to the ERM group to manage those risks," Lefler adds.

Ideally, risk oversight and risk management work together in a continuous cycle, Lefler says. The board systematically identifies and prioritizes risk—whether through audit and risk committees or with the help of consultants. Those findings and decisions are discussed with the CEO and/or the ERM team, which then creates or modifies plans to address the identified risks and presents results to the board. Once the proposed solutions are in place, the board monitors and audits the risk posture of the organization to determine whether the existing processes are managing risk effectively in line with the risk appetite, and the cycle begins again.

Risk Oversight-Risk Management Cycle

The following graphic represents the cycle of risk oversight and risk management. Regardless of where security lies in the cycle, it is incumbent on security leaders to ensure that the significant risks under their purview are being clearly communicated up the chain to inform the board's decision on risk management priorities and resources. Likewise, the security function should have a clear understanding of the corporate risk strategy and appetite as defined by the board and senior management, so that security strategy and operational decisions can follow the board's philosophy. Without this two-way flow of information, neither can be entirely effective.



Analyzing Board-Level Risk Yields Positive Results

Security leaders can enhance their ability to both communicate risk effectively and align with board strategies by learning to see security risks the way the business is likely to see them.

Research by the Security Executive Council has identified common enterprise risks that can be organized into eight descriptive board-level risk categories: Financial, Business Continuity & Resiliency, Reputation & Ethics, Human Capital, Information, Legal, Regulatory Compliance & Liability, New & Emerging Markets, and Physical/Premises & Product.

Security leaders can learn by attempting to group every identified security risk, as well as all security programs and initiatives, into one of those categories. (Note that all organizations are unique, and more or fewer categories may be used depending on industry and size.) This grouping can also be compared to the critical organizational risks the board has identified. This way, the security function can present a direct link between each business category and the potential use of a security program to mitigate the risks identified. It can lead to a number of positive results:

1. Improved communication. Because the flow of information is critical to effective risk management and effective risk oversight, it behooves the security leader to communicate risks and solutions in a framework with which the board is already familiar. Grouping risks in board-level categories creates this framework, ensuring the information presented can be easily understood.

2. A business-first perspective. Any business unit can easily become so mired in its own operations, requirements and challenges that the broader goals and needs of the enterprise become obscured. This exercise enables security leaders who fall victim to

such a mindset to break out of their narrowed view and see their function through the eyes of the business.

A business-first perspective is crucial if the security leader is to honestly answer questions such as, *"If certain security programs do not easily fit into one of the board's risk categories, do they represent an appropriate use of resources?"* or *"Is security neglecting to manage any aspect of the risks the board has identified as critical?"* Questions like these must be answered in order for security to align with business strategy, and they are best answered before the board asks them.

3. Value identification. When security initiatives are presented in the context of board risk categories, the board may benefit from a clearer view of how and where security adds value to the organization. In addition, the analysis may uncover untapped opportunities for security to help reduce redundancies, assist other functions, or expand programs to create new value. In this regard, well-documented metrics provide enormous value to all parties.

4. Strengthened support. The Security Executive Council helps conduct board-level risk analyses based on its research of corporate enterprise risk assessment plans and strategies. Security leaders who have undergone this analysis report that displaying the risks in line with the values of the board helps them gain support and move initiatives through the organization.

Challenges in Board Risk Management

The security function will encounter several challenges to managing the identified board-level risks, particularly where the lines of communication are weak or where the board's interest in risk oversight is aesthetic or shallow.

If the board has not communicated the enterprise risk appetite and priorities effectively, the security leader may glean some knowledge by studying the organization's 10-K statements, if it is a public company.

One challenge to board-level risk management, according to Lefler, is found in the increasing number of business functions being performed by third parties. "From that point of view, a lot of your risk lies with somebody else's employees, goods and services," Lefler says. "The radical shift is that you are now managing risk relationships as opposed to managing the risks themselves."

Security's responsibility shifts from vetting internal employees, for instance, to working with Legal to develop contracts that limit the risk exposure presented by contractors who are vetting their own hires. The security leader must now act as an agent of influence—not only on his or her own senior management, but on the management of the contracted manufacturer.

“This flattening of organizations has resulted in employees and security managers being constrained from resourcing the management of identified risk,” Lefler says. “There is tremendous pressure on security leaders to properly manage identified risk exposure, but the economic downturn has significantly impacted the available resources to address problems. This has required security to reach out rapidly to find service providers for cost-effective solutions to risk issues. That is very challenging.”

However rough the road may be, managing risk in alignment with board priorities is not only a worthwhile goal but a crucial one. There is no evidence that the board’s emphasis on risk will abate; in fact, it is quite the opposite.

Security leaders who have not already begun to shift their thinking and their strategies in this direction may find themselves quickly falling behind.

By considering their place in the oversight-management cycle, analyzing security risks in a board context and confronting board risk management challenges, security leaders can better serve their organizations and perhaps enhance their job security.

Originally Published in Security Technology Executive

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/