By Marleah Blades

Balancing Board-Level Risk

How to ensure your risk management goals align with upper management priorities

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 the new 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 new 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.

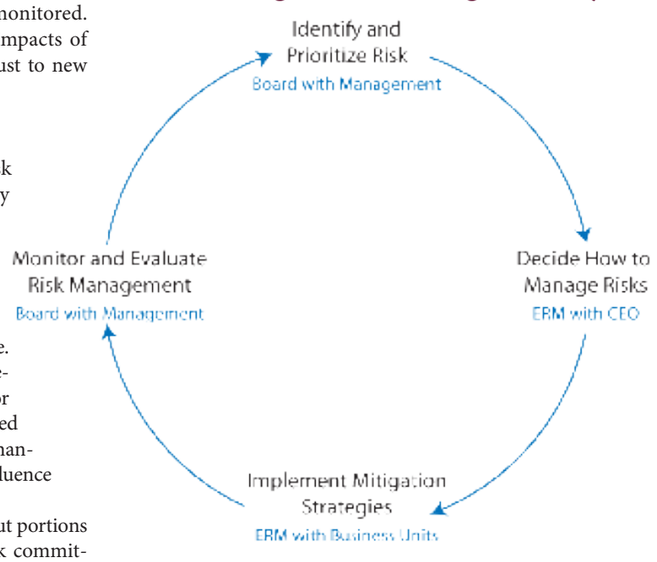
The full board is responsible for risk oversight, but portions of it are generally handled by board audit or risk committees, which are increasingly being assisted by outside parties, says Dick Lefler, former vice president and CSO of American Express and current Chairman and Dean of Emeritus Faculty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



Regardless of where security lies in the circle above, 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 a number of 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. Kenneth Kasten, formerly with Carlson Companies and now emeritus faculty with the Security Executive Council, has analyzed the identified risk factors of 10-K statements for more than 40 organizations and has found some broad commonalities in risk concerns.

"Protection of customer data is one issue many companies recognize as a significant risk," Kasten says. "Those companies whose offerings are intellectual are more likely to emphasize the protection of ideas — patents and such. Manufacturing companies seem to focus more on the protection of physical assets and property. Those who offer a service are more inclined to stress the need for business resilience, and those offering a product are more likely to express a concern about upstream suppliers, downstream vendors and partners whose performance impacts product delivery."

Kasten cautions that not all 10-K risk factor statements are created equal. "Some companies have done a good job with embracing the intent of the document by acknowledging ownership of risk and providing specific, meaningful and actionable comment; while other companies are not quite there yet," he says. "In either case, there is ample opportunity for security leaders to support company efforts with 10-K risk identification, clarification and mitigation."

Another 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. ▮

Marleah Blades is Senior Editor for the Security Executive Council (SEC), a problem-solving research and services organization focused on helping businesses effectively manage and mitigate risk. The Council provides strategy, insight and proven practices that cannot be found anywhere else. For information or comments on board level risk issues, e-mail contact@secleader.com. Follow the Council at securityexecutivecouncil.com, or on Facebook and Twitter.

The Risk and Uncertainty Initiative

The University of South Carolina's Moore School of Business is currently developing a Risk and Uncertainty Initiative that will bring together faculty and experts from a variety of disciplines to address the challenges of risk and uncertainty management in business.

The initiative, which will be consistent with an enterprise risk management approach, will tackle issues that are relevant to the current business climate, says Greg Niehaus, Professor of Finance and Insurance for the Moore School. "The events of the last four years have done nothing but bolster the importance of risk and uncertainty management," he says. "The Initiative will facilitate interaction among faculty across a wide range of disciplines and between faculty and business leaders. It will also support research on risk and uncertainty issues and hopefully influence the curriculum of our degree and executive programs. Ultimately, we want to influence the practice of risk management."

The initiative will also complement the Moore School's international reputation — it boasts the nation's top undergraduate international business program and the number two spot in U.S.News & World Report's 2012 ranking of international graduate business programs.

"Risk management is and has to be much broader than finance and insurance," says Niehaus. "It is part of decision making within an organization at every level and in every area. I don't think it's been emphasized enough how to properly incorporate risk into decision making, and hopefully the Risk and Uncertainty Management Initiative will work to correct that."