By Marleah Blades

Is ERM Leaving Security Behind?

Ideally, enterprise risk management (ERM) is a top-down, formal framework for identifying, prioritizing, analyzing, monitoring and managing all types of risk that an enterprise faces. It provides solid guidance for executive decision-making. It is headed by the strong leadership of a B-level or C-level officer and it enjoys the enthusiasm and involvement of the board and the entire executive team. It is founded on a clear articulation of the company's risk appetite — aligned with business goals — that is communicated to employees at all levels. It is supported by a cross-functional management and advisory team that shares information about business unit risk.

In a perfect world, ERM would save the company money, prepare it for change, create stakeholder value and facilitate growth through the exploitation of opportunities. All organizations would be interested in and capable of embracing some sort of ERM model to manage risk, and the security function would play a weighty role in the process.

It's a shame the real world seldom lives up to such ideals. ERM — developed with top-down support and strong leadership — can indeed lead to benefits like those mentioned above. But organizations have been slow to adopt it, and those that have climbed on board do not always invite security to help steer.

Not Yet Widely Accepted

In its April 2009 "Report on the Current State of Enterprise Risk," the ERM Initiative at North Carolina State University stated that 44 percent of 700 survey respondents

(most of whom were CFOs) have no enterprise-wide risk management process in place and have no plans to implement one. IBM announced similar findings in its 2008 CFO Study, reporting that only 52 percent of CFOs surveyed have a prescribed risk management program.

What's more, the NC State report found that nearly half of respondents lack a formal plan for business functions to establish or update assessments of risk exposures, and 75 percent indicate that key risks are communicated "merely on an ad-hoc basis at management meetings."

These days, it is common knowledge that companies collapse when they make the wrong decisions about risk; we have learned that courtesy of the economic crisis and the behavior responsible for it. If we all know this, why is enterprise risk management still not the norm?

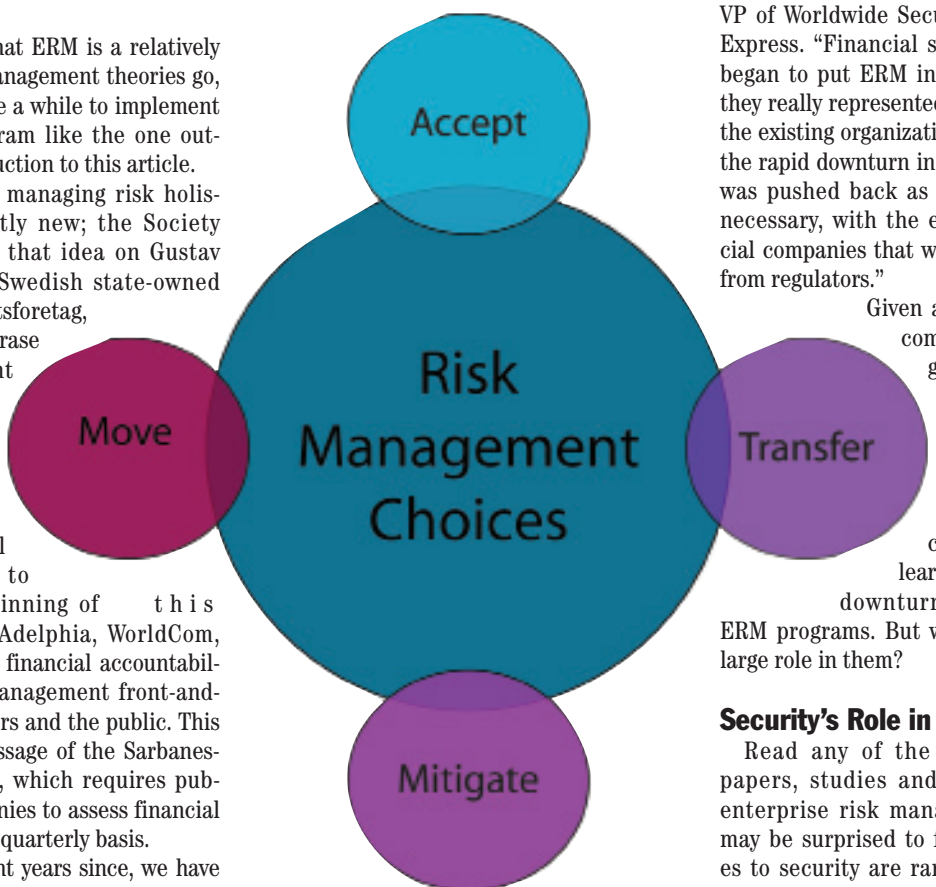
Why So Slow?

One reason is that ERM is a relatively new concern as management theories go, and it tends to take a while to implement a total ERM program like the one outlined in the introduction to this article.

The concept of managing risk holistically isn't exactly new; the Society of Actuaries pins that idea on Gustav Hamilton of the Swedish state-owned holding group Statsforetag, who coined the phrase "risk management circle" in the 1970s. But the idea of ERM as a formal framework didn't really take off until scandals began to break at the beginning of this decade — Tyco, Adelphia, WorldCom, Enron — bringing financial accountability and risk mismanagement front-and-center for legislators and the public. This resulted in the passage of the Sarbanes-Oxley Act in 2002, which requires publicly traded companies to assess financial reporting risk on a quarterly basis.

In the scant eight years since, we have seen the release of additional Securities & Exchange Commission guidance on risk assessment, the development of formal ERM frameworks like the COSO Enterprise Risk Management Integrated Framework, the launch of a family of risk management standards (ISO 31000), and the announcement that Standard & Poor's would begin evaluating ERM as part of their credit rating process for both financial and non-financial corporations. That's a lot of action in a little time.

A quick note: Many of the events and actions that drove the increased visibility of ERM were strictly or predominantly focused on direct financial risk. For instance, SOX requires risk assessments, but it truly concerns itself with risks to accurate financial reporting. ERM in its ideal is bigger than such compliance risk assessments, taking into account not only financial risk but operational risk, strategic risk, reputational risk, hazard risk, etc. I believe the Casualty Actuarial Society puts it best: "Enterprise risk is a 'big idea.'" Despite these facts, some organizations limit their practice of it to direct financial issues. More on that later.



Senior Management has four options in managing risk: to accept it and do nothing; to transfer it (by purchasing insurance, for instance); to move it or move from it; or to mitigate it.

A second reason for the delay in ERM implementation is that companies that see the value in formal, top-down ERM programs often face an uphill battle to accomplish the kinds of cultural shift and structural change necessary to implement them.

This battle is complicated by the fact that, according to Chief Executive Magazine, the typical tenure of a CEO is between four and five years. That means that a CEO may recognize the importance of ERM and work with his or her executive team to realize it, only to be replaced shortly thereafter by another CEO who has less interest in nurturing the program.

Yet another complication: the economy. "Companies are struggling with their costs right now. Many can't afford to roll out new programs," says Richard Lefler, dean of emeritus faculty for the Security Executive Council and former VP of Worldwide Security for American Express. "Financial services companies began to put ERM in place rapidly, but they really represented a consolidation of the existing organizational function. With the rapid downturn in the economy, ERM was pushed back as desirable, but not necessary, with the exception of financial companies that were under pressure from regulators."

Given all these obstacles, companies can be forgiven for the slow ERM acceptance rate. The hope is that as the economic forecast brightens, more companies will learn the lessons of the downturn and implement ERM programs. But will security play a large role in them?

Security's Role in ERM

Read any of the numerous white papers, studies and examinations of enterprise risk management, and you may be surprised to find that references to security are rare and fleeting. To the security leader, this may make little sense. Security is all about risk. Why does it seem as though corporate security is hardly involved in ERM? Shouldn't corporate security be a major source of support for an ERM program, at the least?

Perhaps in some cases it should, but that is not how most corporate executives see things. Various studies have found that, while several financial companies have appointed Chief Risk Officers to lead risk management programs, many other organizations have put the CFO at the head. The CSO does not appear to be in the running. Again, there are a variety of reasons for this.

Residual risk is the risk that remains after inherent risk (threats and vulnerabilities) is offset by control risk (proactive, prevention focused risk mitigation).

For one thing, as mentioned above, many companies look at ERM as primarily a device for managing financial risk, so their risk management programs — even those under the ERM moniker — may not exactly be enterprise-wide. NC State's "Report on the Current State of Enterprise Risk" found that 19 percent of the audit committees that formally monitor risks for the board of executives only monitor financial risks; 63 percent monitor operational and compliance risks in addition to financial risks; and only 18 percent monitor all entity risks.

This is a misstep on their part, since a Corporate Executive Board study found that non-financial risks accounted for 85 percent of the risk types that led to companies' market capitalization decline of 30 percent or more. "Security has a critical role in ERM as it manages mitigation programs protecting employees, investments and the brand," Lefler says. "Of equal importance but seldom discussed is the residual risk that security manages — for example, the 24-hour security center which not only manages security exposure but is often the first to be notified of a critical event impacting the company. Proper notification procedures on emerging events (including critical incidents, world crisis events, and potential business continuity issues) reduce the exposure of the company and improve the response of all units." Clearly, ERM is not all about money and should not be treated as though it is.

That said, ERM is all about money, in another sense. The point of managing risk is to avoid failure or damage (which costs money) and to find opportunities (which make money). ERM is about prioritizing risk to match business goals, and the sad fact is that for most companies, security is not. Security is still about saying no to new ideas without regard to risk appetite, being the corporate cop. And because of that, Lefler says, "business executives don't necessarily see the importance of security mitigation programs in helping them accomplish their goals. Many of the financial services companies do — especially where it comes to controlling fraud and insider threat. But a lot of other companies really don't yet visualize the possibilities that ERM with security inclusion can mean to achieving their business goals."

Lynn Mattice, Chairman of the Board of Advisors for the Security Executive Council and former VP and CSO of Boston Scientific, adds, "For a security function to work properly and provide the kind of intelligence that allows the company to effectively leverage its markets and manage its risk portfolio, you've got to understand the business environment, the supply chain, the political issues you'll be facing, all the different risks you're up against; and to be able to deal with the kinds of problems, disruptions and opportunities that exist across the globe. If you don't have a handle on that, you've got no ability to understand how events and risks will impact the company."

Put on Your Business Hat

The disconnect between security and ERM shows where security has missed

Risk Management Silos vs. ERM

By Richard Lefler

Right now, many organizations manage risk at the silo level. Take IT security, for example. IT security often reports to the CTO or CIO and decisions are made within that silo about protecting the company's information. Those decisions may not be fully appreciated or understood by business leaders. The risk there could be extraordinary.

A recent major retailer case is a classic example. The CISO at the retailer went to management and said, "We need to go to a second level of encryption in our point-of-sale devices at stores." They said no. The impact of the publicity when their system was compromised and millions of their customers' credit card information was compromised was extraordinary, and the subsequent cost to their company was enormous.

It raises the question of whether the businesspeople would have approved the cost if there had been an ERM team looking at the holistic exposure to the company. The silo decision created exposure to the retailer across all business units and departments; the risk exposure went far beyond a data compromise at a store.

In order for risk management in an organization to be holistic, it has to be led at a high enough level that the people managing it can see it across the enterprise. The function of this C-level executive is to manage the team by pulling together existing silos that manage risk and forcing a holistic look at what the risks are to the company at the highest levels.

Richard Lefler is former CSO of American Express, and is currently Dean of Faculty for the Security Executive Council.

its opportunity. "We made a huge mistake years ago in the security arena. We had an opportunity to grab the title 'risk management' — because that's really what corporate security functions are all about: identifying risk, analyzing risk and providing viable mitigation solutions within the risk tolerance level of the organization," Mattice says. "But instead we chose to hold on to security as an age-old link to law enforcement." Security is missing its chance to be a change agent, to gain executive stature in the organization, and thus to provide better value in organizational security.

NC State's "Report on the Current State of Enterprise Risk" found that 19 percent of the audit committees that formally monitor risks for the board of executives only monitor financial risks; 63 percent monitor operational and compliance risks in addition to financial risks; and only 18 percent monitor all entity risks.

ERM will continue to grow in acceptance. NC State's report noted that almost half (45 percent) of respondents said the board of directors is asking senior executives to increase their involvement in risk oversight.

"Unless the role of the security function can be clearly defined and the value of it effectively articulated, it's never going to be deeply engaged in ERM," Mattice says. "We need to do two things: 1) get senior executives educated about the value proposition that a well-functioning security/business intelligence organization can provide to the company in helping it understand and manage its global risk portfolio; and 2) get corporate security executives to focus on how they align with the business and be able to understand and respond to the needs of the business."

Mattice believes corporate security functions will continue to be marginalized in ERM unless security leaders begin looking at themselves as business leaders and acting accordingly. ▮

Marleah Blades is senior editor for the Security Executive Council. For more information, visit www.securityexecutivecouncil.com/?sourceCode=std.