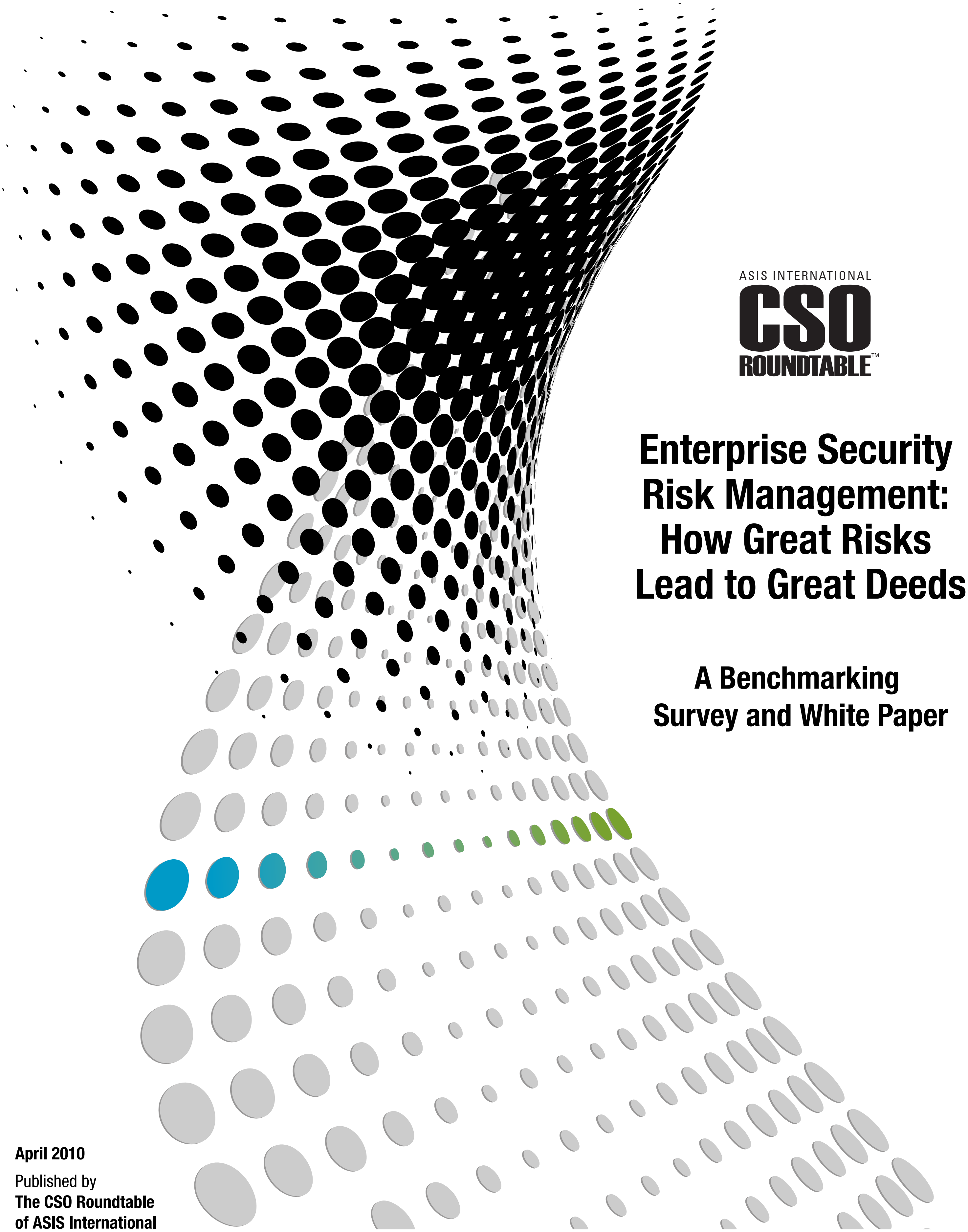


ASIS INTERNATIONAL
CSO
ROUNDTABLE™

Enterprise Security Risk Management: How Great Risks Lead to Great Deeds

A Benchmarking Survey and White Paper

April 2010

Published by
The CSO Roundtable
of ASIS International

ASIS INTERNATIONAL
CSO
ROUNDTABLE™

The CSO Roundtable provides a dedicated forum for the senior-most security professionals from the largest and most influential organizations in the world. An initiative of ASIS International, the CSO Roundtable became its own membership organization in 2008 to gain recognition for and enhance the standing of the CSO position; to assist CSOs in job performance, leadership, and professional development; and to develop the next generation of corporate CSOs.

The CSO Roundtable would like to extend its sincere thanks to the members of its Enterprise Security Risk Management (ESRM) Working Group, whose expertise and guidance made this survey and white paper possible. Some members of the group wished to remain anonymous and are not listed below.

Brian Allen, CPP, Senior Director Corporate Security, Time Warner Cable, USA
Walter Fountain, CPP, Director Enterprise Security, Schneider National Inc., USA
Daniele Gulinatti, Security Director, Telecom Italia Mobile S/A, Brazil
Simon Hoyle, Vice President Risk Management, Majid Al Futtaim Properties, UAE
Petri Lillqvist, Director Risk Management, Digita Oy, Finland
Joseph McDonald, CPP, PSP, Chief Security Officer, Switch Communications Group, USA
RC Miles, CPP, Head of Global Security and Business Continuity, Life Technologies Corporation, USA
Dick Parry, CPP, Executive Director, Global Security, Novartis Institutes for BioMedical Research, USA
John Petruzzi, CPP, Senior Vice President, Andrews International, USA
Kevin Richards, CISSP, President, ISSA International, USA
Dave Tyson, CPP, Chief Information Security Officer, Pacific Gas & Electric Company, USA
Richard E. Widup, Jr., CPP, CFE, Senior Director, Corporate Security, Purdue Pharma L.P., USA
Timothy Williams, CPP, Director of Global Security, Caterpillar, USA

Enterprise Security Risk Management: How Great Risks Lead to Great Deeds

Introduction

More than two millennia ago, the Greek historian Herodotus wrote, “Great deeds are usually wrought at great risks.” How important and accurate those words are even centuries later, as risks have become vastly more complex. Herodotus’ words underscore a vital concept of business: that risk, whatever it may be, must be understood and managed to achieve a positive outcome. Business executives understand that risk brings opportunities as often as it brings danger—but security executives have traditionally not seen risk in this light. Indeed, with good reason security has always focused on the danger and not the opportunity.

That perspective has undergone an important change. Security professionals like myself have long struggled to make business leaders view security as a profit center, not an expense, in part by emphasizing the cost of what could happen if risks were ignored. This strategy has had limited effectiveness, for three related reasons. First, we often tended to overlook the “opportunity” side of risk, meaning that we couldn’t demonstrate how to add to the bottom line. For example, would a security department typically claim to have added value to a profitable acquisition if it assisted with due diligence and gave its imprimatur to the deal? I doubt it. Second, even if they did, how could they measure or quantify that success? Third, many of us simply didn’t understand precisely how our organizations made money, and therefore how security could add to the bottom line. These situations arose from the same cause: Many security professionals, while top experts in their fields, had inadequate business skills. We simply couldn’t fluently speak the language spoken in the C-suite, and many of us, I’m afraid, didn’t make a strong effort to learn it.

As I said, that has changed dramatically. During my career I have seen new generations of security professionals who understand business as well as they understand security issues. In fact, I often hear from these leaders that they’d rather have a business person than a security person as a deputy; a business person can more easily learn security than the other way around. I’ve been proud to be someone who understands both security and business—I simply couldn’t have succeeded as CSO of a Fortune 100 company if I weren’t. And I’m proud that ASIS International has been a driving force behind that change in perspective.

Years ago, ASIS began reaching out to other security associations as part of a collaborative effort to create an integrated approach to identifying and mitigating all the risks that organizations face. This effort was dubbed enterprise security risk management—ESRM. With ESRM’s holistic approach to security came the understanding that a whole host of business issues that were not traditionally associated with “security”—think, for example, of Sarbanes-Oxley or HIPAA—were now firmly part of security’s bailiwick, underscoring again how important it is for security professionals to be business professionals first.

When the CSO Roundtable, a membership group within ASIS of the most senior security executives from the world’s largest organizations, began the ESRM benchmarking survey you now have in front of you, the goal was simply to discover how widespread this holistic-security idea is, and what ASIS could provide to advance it. The survey was sent to more than 200 members of the Roundtable, and then to the ASIS membership. The results are truly noteworthy, shedding much-needed light on security and risk.

We've learned that traditional security issues are rarely the ones that are keeping security professionals awake at night; instead, risks such as database theft, network failure, and economic problems are top concerns. We've discovered that most CSOs, and indeed nearly half the non-CSOs, are already deeply involved with evaluating and mitigating nonsecurity risks in their organizations. And we've found that the vast majority of security professionals believe that excellent business management, leadership, and communication skills—not security expertise—are the traits that will lead to success in ESRM, and ultimately in the board room.

The exuberant response to the survey makes it clear that ESRM is a subject that security professionals crave more information about. Respondents told us they wanted to know how security executives have been able to successfully implement ESRM initiatives, and they wanted as many details as possible. So the Roundtable selected nearly a dozen CSOs and CISOs from around the world who have led or are in the process of leading ESRM programs, and picked their brains. The result was *How Great Risks Lead to Great Deeds*, which digs deeply into these initiatives and shares, warts and all, what went wrong and what went right.

This benchmarking survey and white paper will serve as a snapshot of how well security professionals understand ESRM, what the challenges of its implementation across an entire organization are, and precisely what the rewards are. For the business, rewards include ensuring that a broad range of risks—including those to areas that aren't always considered by corporate "risk management" practices, such as reputation and brand—are reviewed with an expert eye. And for the security professional, the rewards include a better understanding of the business, which can significantly enhance a career.

I'm grateful to those who shared their experiences and ideas to make this survey and paper so enlightening and important. Security professionals know better than anyone that the world is a risky place—we've dedicated our lives and careers to being the bulwark against those risks. By working closely together with our colleagues across the organization, we can do an even better job of safeguarding people and property. But we can also do a better job of helping our organizations grow and be successful. Only when we understand and appreciate all the risks that organizations face, regardless of where they come from or who is the first line of defense, can we ensure that great deeds will follow.

Timothy Williams, CPP
Director of Global Security
Caterpillar

Enterprise Risk Management Reborn: Creating Value

In December 2009, TIME magazine declared the 00s the "Decade from Hell." Bookended by the 9/11 terrorist attacks, the anthrax episode, and Enron at one end and the global financial collapse on the other—with a series of unprecedented catastrophic hurricanes and floods in the middle—the first years of this century will very likely be seen as the most daunting decade Americans have lived through in the post-World War II era. Is this an omen of what the 21st century has in store for us? Most likely.

One of the hallmarks of the twenty-first century will indeed likely be more and more unthinkable events, previously unseen contexts, and pressure to react extremely quickly, even when we cannot predict the cascading impact our actions might have. That is because the world has been evolving at an accelerating speed. These changes have brought many positive developments. We all benefit from globalization of social and economic activities. Communication costs are close to zero, goods and people travel faster and more cheaply than ever before, and knowledge is shared with unprecedented ease on the Internet.

Yet the flip side of this extraordinary transformation has been somewhat overlooked: Actions taken or risks materializing 5,000 miles away can affect any of us very soon thereafter. Viruses fly business class, too! The litany of global interdependent risks is almost endless. Events that have surfaced prominently on the social, economic, and political fronts in many countries just since the beginning of 2001 are eye-opening: financial crises; global warming; scarcity of water and other resources; hurricanes, floods, earthquakes, and other natural disasters unprecedented in scale and recurrence; nuclear threats; pandemics and new illnesses; failures of our aging critical infrastructures; security breaches and large-scale data thefts; and so on.

That the Annual Meeting of the World Economic Forum in Davos devoted several sessions on this global risk management issue in 2009, and even more in 2010, is a perfect indicator of our changing world. In this context, establishing a strong enterprise security risk management strategy should not be viewed by corporations as a costly luxury: to the contrary, it has become a necessary condition to create sustainable value to the shareholders—if not to simply survive.

The irony is that, as a result, security has become too important to be handled by security experts alone. As risks and opportunities are becoming larger in scale and we all face growing uncertainty, the question of how to move successfully from "security as a cost" to "creating value from security" is now facing corporate executives in the C-suite. This poses daunting implementation challenges, as Timothy Williams rightly notes in the introduction of this report. The results of this innovative ASIS International/CSO Roundtable initiative have to be seen in that broader context.

The growing recognition of Enterprise Security Risk Management (ESRM) as a holistic view of risk—all risks—throughout an organization is important; this holistic view helps ensure that the threats that might typically not be recognized in an enterprise risk management program focusing primarily on financial risks (such overlooked risks, for example, might include: risks to brand and reputation; physical supply-chain risks; or loss of consumer confidence if your data is stolen or networks attacked) are now more and more fully identified, prioritized, and mitigated. These are lessons referred to in the survey and white paper.

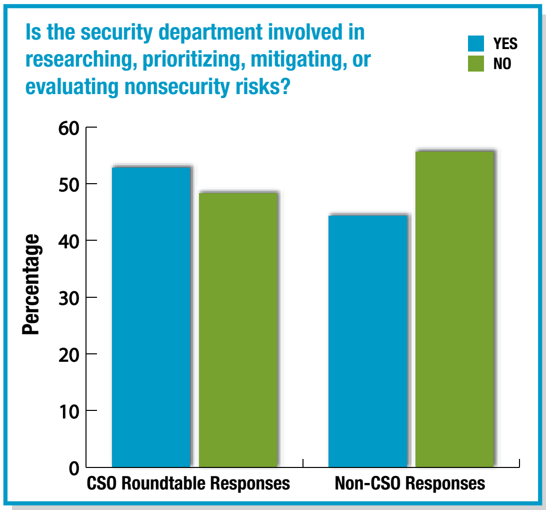
This is why this first ESRM benchmarking survey, along with the lessons-learned white paper, helps prepare the groundwork for future research into this area. For sure, leading international institutions such as the Wharton School will benefit from these new insights as we teach all our students how to best prepare to lead the world of tomorrow. We look forward to a long-term working relationship among the School and the leading actors of this new security environment.

Dr. Erwann O. Michel-Kerjan
Managing Director, Risk Management and Decision Processes Center, The Wharton School
Chairman, OECD Secretary-General Advisory Board on the Financial Management of Catastrophes
Member of the Global Risk Network, World Economic Forum

Enterprise risk management (ERM) looks at the universe of risks—financial, strategic, accidental, and so on—that an organization faces. However, ERM does not always fully take into account the risks that are traditionally associated with security. Enterprise security risk management (ESRM) exists to ensure that these risks are properly considered and treated.

ASIS International, the world's leading organization for security professionals, recognizes that ESRM is key among the opportunities and challenges in security and has consistently included ESRM in its annual strategic plan, with goals of advancing the understanding of ESRM among members and developing networking and educational opportunities that will assist security executives in deploying ESRM initiatives. To reach those ends it was important to first benchmark the membership's understanding of ESRM by creating a membership-wide survey.

In October 2009, the CSO Roundtable of ASIS International, a membership group of the senior-most security executives from the world's largest organizations, launched a comprehensive ESRM survey to its members and then to the membership of ASIS. The survey asked for information about what risks were the most challenging; where organizational support for ESRM initiatives came from; which business elements were included; what security's role is; who has ultimate responsibility for risk; and other benchmarking questions. More than 80 chief security officers, and over 200 ASIS members, responded to the survey. Here's what security professionals had to say about ESRM.

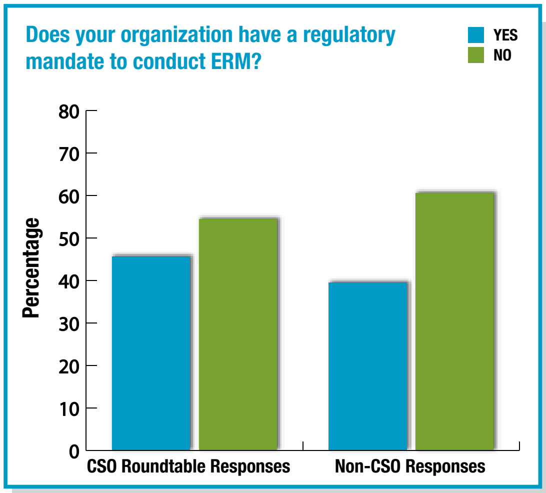

Is the security department involved in researching, prioritizing, mitigating, or evaluating nonsecurity risks?

Security's Role in Risk Assessment and Mitigation

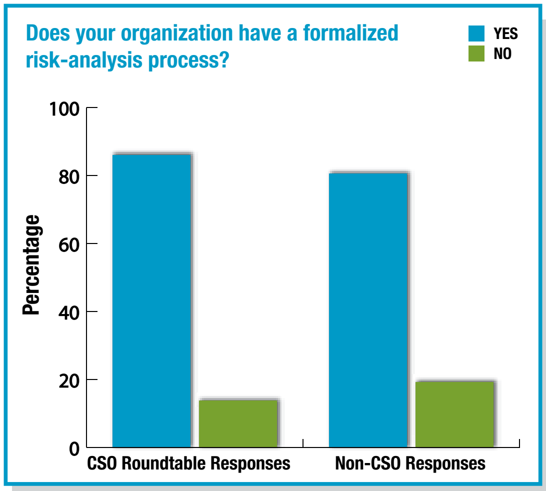
- **What are the three greatest nonsecurity risks facing your organization?** For CSOs, the greatest nonsecurity risk was the downturn of the economy, followed by business issues such as competition and regulatory pressures. For non-CSO respondents, the top nonsecurity concerns were IT-related, in particular database compromise, the failure of data networks, and the inability of their organizations to keep up with current technology and threats.

- **Is the security department involved in researching, prioritizing, mitigating, or evaluating nonsecurity risks?** CSO Roundtable members are more likely to be involved with evaluating and mitigating nonsecurity risks than the rest of the ASIS membership. Still, nearly half of all respondents said they are involved. About a quarter of all respondents noted that their departments have specific "risk assessment" responsibilities.

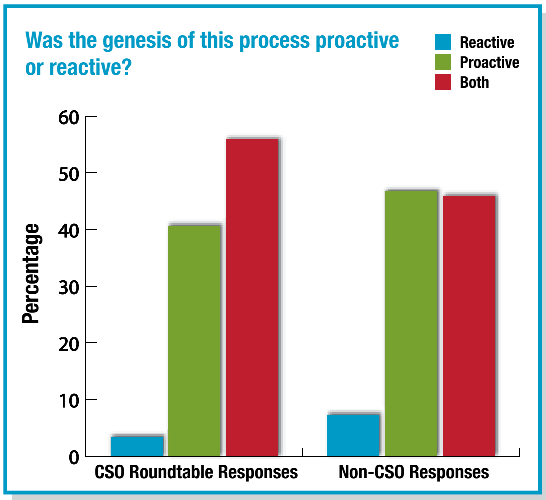
- ***Does your organization have a regulatory mandate to conduct ERM?*** Nearly half the CSOs, and about 40 percent of non-CSO respondents, said their companies have such a mandate.


Does your organization have a regulatory mandate to conduct ERM?

- **Does your organization have a formalized risk-analysis process that includes the identification and prioritization of risks and the development of an action plan? If so, what is the security department's role in this effort?** Nearly 90 percent of CSOs, and 80 percent of non-CSOs, said that their organizations have such a process. CSOs said security's role included: physical asset and employee protection; emergency preparedness and planning; occupational safety; and business continuity. Many CSOs said they either lead the effort or are active members of a larger ERM team. One noted that security serves as a "constant reminder to others that there is a level of risk assumed in all business evolutions and that all risk needs to be addressed."

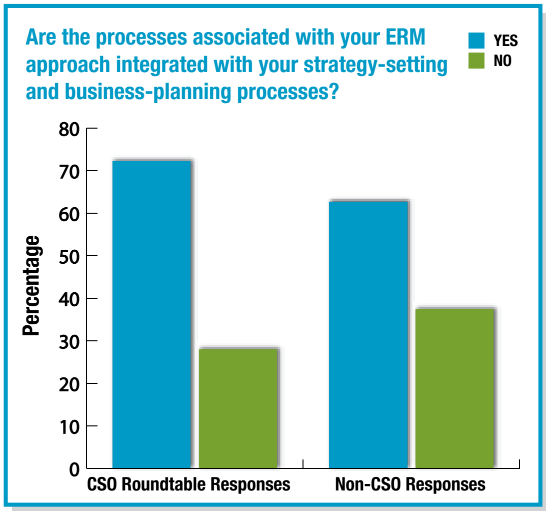

Does your organization have a formalized risk-analysis process?

- **Was the genesis of this risk-analysis program proactive (because this is considered a best practice), reactive (caused by a particular incident or incidents), or both?** Very few respondents—less than four percent of CSOs and about seven percent of non-CSOs—said their programs were reactively created. Non-CSO respondents said their programs were proactive more often than CSOs did (47 percent vs. 41 percent), while CSOs were more likely to have a program that was a combination of proactive and reactive in nature (56 percent vs. 46 percent).


Was the genesis of this process proactive or reactive?

- **What terminology is used in your organization for risk management (e.g., "enterprise risk management," or "ESRM," or something else)?** Nearly 40 percent of CSOs, and more than half of non-CSO respondents, said their organizations term their risk-analysis program "risk management" of some form (including "security risk management," "company risk management," or "operation risk management"). More than a third of CSOs said their programs are called "ERM" while more than one-quarter of non-CSOs said the program is called "ERM."

- **Are the processes associated with your ERM approach integrated with your strategy-setting and business-planning processes?** Nearly three-quarters of CSOs said that the processes used for enterprise risk management strategy were integrated with their organizations' strategy-setting and business-planning processes. About two-thirds of all respondents indicated their processes were so aligned.


Are the processes associated with your ERM approach integrated with your strategy-setting and business-planning processes?

- **How often are these processes integrated, evaluated, and/or realigned if necessary?** Almost one-third of CSOs, and nearly half of non-CSOs, said their ERM processes are integrated with their organizations' strategy-setting and business-planning processes annually; about 20 percent of CSOs and non-CSOs alike said this was done quarterly.

- **What elements of security-related risk are incorporated (for example, business continuity, IT security, brand protection, etc.)?** Business continuity and IT security were the two main elements of security-related risk incorporated into the risk-management strategy for non-CSOs; more than half mentioned IT, and almost two-thirds mentioned business continuity planning. CSOs swapped those figures: Nearly 60 percent of CSOs said IT was incorporated into their risk management strategy, with 52 percent saying business continuity. Almost a quarter of CSOs noted that brand protection was part of this strategy.

- **What are the security department's roles and responsibilities in the risk management effort?**

  a. Responses from CSOs included:

  i. We participated with the rest of the organization in identifying the enterprise risks. We take an active role through our strategic and business plans in moving initiatives and measures to eliminate or mitigate the risks applicable to security.

  ii. Corporate security evaluates the security framework of the company and informs business units and top management about any significant changes.

  iii. Security is a risk-governance function mandated to ensure, advise, assess, and partner the management of security and geopolitical risks.

  iv. We own it.

  v. The CSO is a CEO direct report and manages the security risk management process via coordination with all departments, and by maintaining the emergency management plan, continuity of operations plan, security strategic plan, security metrics, and reporting.

  vi. When the risk department identifies a threat that falls into the security arena, we address the issue and propose solutions.

b. Responses from non-CSOs included:

i. The security department is solely responsible for all risk-related matters.

ii. Security is intimately involved in the overall analysis, planning, and implementation of risk-related mitigation strategies.

iii. Managed by CIO office. All security is included under its umbrella.

iv. Evaluate/assess various threats to critical infrastructure and assets, host regular meetings/trainings and exercises, provide information, and manage community-security partnership programs.

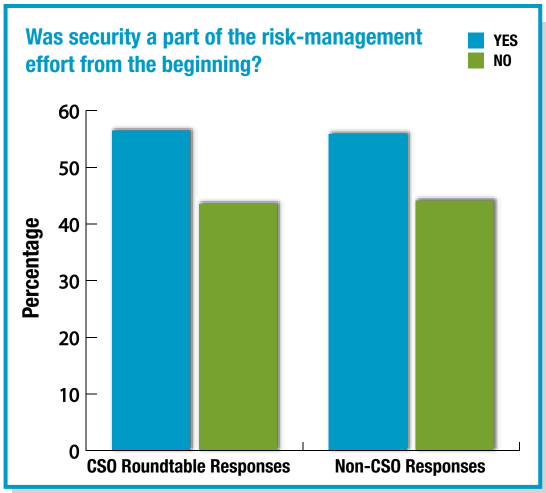
v. At this time, the security department is limited to physical site reviews and security recommendations.

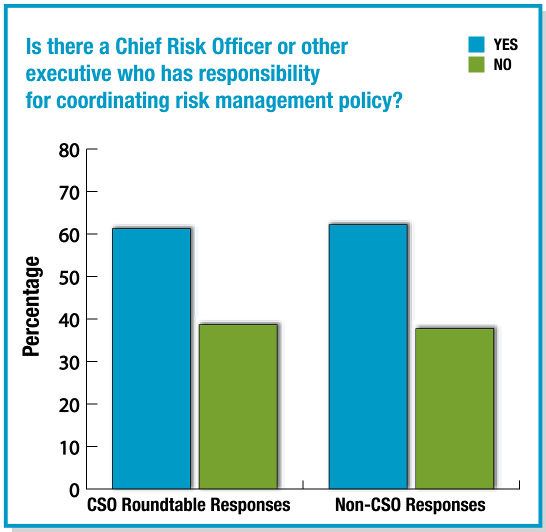
vi. Security is responsible for the protection of persons and property, emergency management, initiating business continuity planning, and overseeing security for backup locations. Only recently is security involved with audit and risk in assessing internal processes and controls for other departments.

- **Was security a part of this effort from the beginning?** Nearly 60 percent of both CSOs and non-CSO respondents said that security was a part of the risk management effort from its outset.

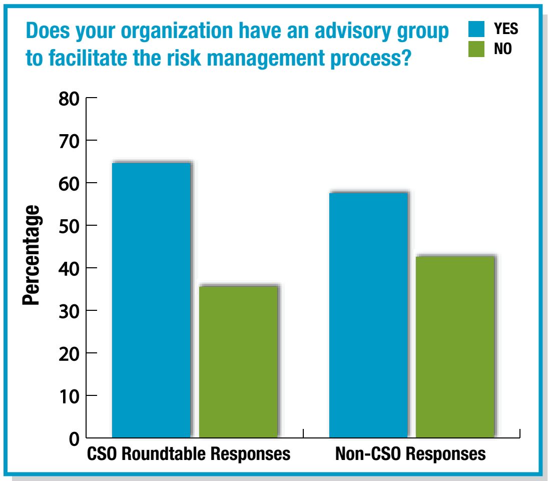
- **Is there a Chief Risk Officer or other executive who has primary responsibility for coordinating risk management policy, execution, and reporting? To whom does this person report?** Nearly a quarter of CSOs said it was the organization's CEO who held this responsibility; about 21 percent said it was the CFO; and about 11 percent said it was legal counsel. Six out of 10 non-CSO respondents said their organizations have a CRO or other executive responsible for this.

- **Does your organization have an advisory group that cuts across different departments to facilitate the risk management process?** CSOs were more likely to have a cross-departmental advisory group on risk management than the general membership, with nearly two-thirds responding that they have such a group compared with about 58 percent of non-CSO respondents.





- **Which departments participate in this group, and how often do they meet?** Most respondents said these groups met quarterly or monthly. A few said they have weekly meetings or calls. Regarding the composition of these groups, answers from CSOs and non-CSOs varied greatly.


Does your organization have an advisory group to facilitate the risk management process?

  a. *Responses from CSOs included:*

     i. Finance, audit, security, and risk.

     ii. Operations, legal, finance, and safety.

     iii. Corporate security, internal audit, information security, insurance, legal, compliance, and the risk control group (concerned with Sarbanes-Oxley).

     iv. All lines of business and shared services are represented.

     v. EO Office, finance, HR, corporate affairs, and security.

     vi. Operations, IT/CIO, information and physical security, legal/privacy, and all lines of business.

     vii. Business operations, technical/science management, legal, HR, IT, security, and safety.

     viii. Legal, controller, internal audit, compliance, security, and executive representation.

  b. *Responses from non-CSOs included:*

     i. Security, safety, human resources, business units, legal, and IT.

     ii. Representatives from all departments.

     iii. Senior management, legal, HR, communications, safety, security, and contracts.

     iv. IT, IT security, general counsel, executive management team member, and corporate security.

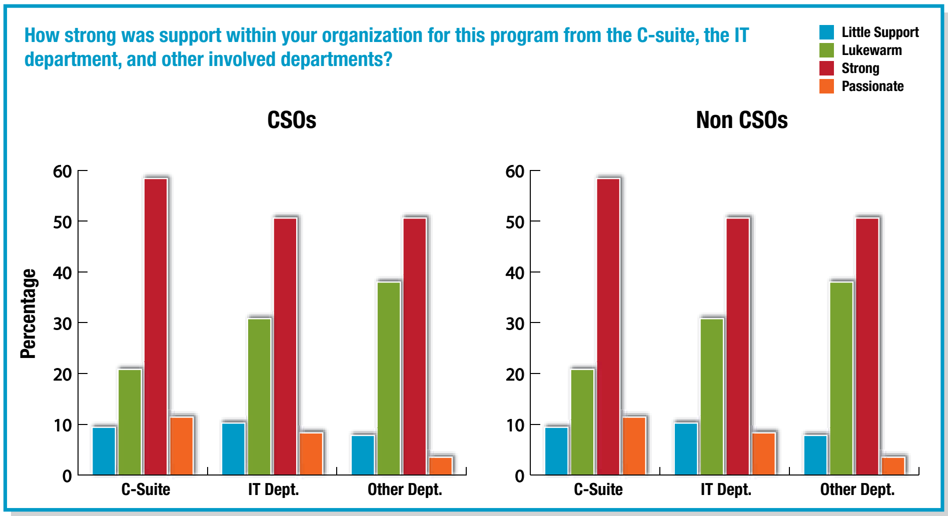
     v. Risk, finance, nursing, physicians, HR, facilities, security/safety, disaster management, infection control, and compliance.

     vi. Security, finance, HR, marketing, technical operations, and engineering.

     vii. Global corporate security.

     viii. Internal audit, marketing, security, legal, finance, customer service and sales, technology (including IT), strategy, HR, and health and safety.

     ix. Infrastructure department heads (human resources, treasury, facilities, IT, safety, security, procurement, and others) comprise a Crisis Response Team.



How strong was support within your organization for this program from the C-suite, the IT department, and other involved departments?

- **How strong was support within your organization for this program from the C-suite, the IT department, and other involved departments?** Support for the ESRM initiative from the C-suite was described by most respondents as “strong” or “passionate” (almost 75 percent of CSOs and almost 70 percent of non-CSOs). About 30 percent of all respondents characterized support from the IT department as “lukewarm,” though more than half of both groups still called IT support “strong” or “passionate.” The area of weakest support came from other departments involved in the initiative. Nearly half the CSOs and non-CSOs said these departments gave little or lukewarm support.

- **What obstacles (organizational, funding, personnel, etc.) have you encountered in making this holistic risk management initiative successful?** Responses from both groups were similar, with funding, personnel, and getting support the most common. Here’s a sampling of what both groups encountered.

  a. *Responses from CSOs included:*

     i. Personnel challenges to keep the risk process fresh and meaningful—same leaders have resulted in very similar results.

     ii. Too much “real” work, too few people to attend to the risk issues.

     iii. None to speak of; make the business case and the firm supports.

     iv. Acceptance that risk is real, not conceptual.

     v. Tendency to overlook security (malicious risks) and to focus on commercial risks.

     vi. Some defense of turf. However, the primary resistance was more benign neglect.

     vii. Perceptions of leadership that risk management is an if-come scenario. It is difficult to prove the value of a negative. If it hasn’t happened yet, why do you think it will? Why should we spend money on something that may not occur?

     viii. Breaking down silos in finance and internal audit departments.

     ix. Budget for staffing. The need was not clearly understood.

     x. Communicating the various forms of risk has not been easy.

xi. Risk Committee output is “business confidential” and “restricted.” This results in poor communication from the top to middle managers making the work of the Risk Committee largely invisible from the rank and file. This causes issues when solutions are required and staff is unsure what is driving the effort.

xii. This is a new concept for them; we get a lot of nodding of heads but little follow up. Working on accountability.

xiii. Funding is always an issue, especially in this economy.

xiv. Collecting information from various stakeholders is time consuming and seen as a competing priority with other business issues.

xv. The major obstacle has been a lack of definition between ERM and ESRM, the definition of what is a security risk, how the two interact, what security’s role is within the ERM process, and the difference between the two.

b. Responses from non-CSOs included:

i. Organizationally, it has been a challenge to find the time among limited resources.

ii. Silo mentality and a “tick and flick” approach due to Sarbanes-Oxley.

iii. Initial buy-in and participation by departments that are too busy to participate (especially in the preparatory and ongoing assessments required).

iv. External regional risk not really integrated with local business/operational risks.

v. It has been very difficult to make this holistic because each business makes an independent decision on how much, if at all, to participate in the enterprise risk management initiative. All businesses participate in the annual audit, but that is all they are required to do.

vi. Funding.

vii. Personnel.

viii. Organizational: the concept is not well understood. Funding: it is very difficult to invest in prevention. Personnel: very few people have the knowledge so there is little support.

ix. Turf concerns have been a major problem. With the economic downturn money has been decreased but is proportional not excessive.

x. No more than usual in similar business ventures that cross functional department boundaries.

xi. Six magic words: “It’s not an issue to me.” The greatest obstacle is management’s attitude of disbelief in dishonest people or employees. We have 28 branches and management still has the “Mom & Pop” approach to business.

xii. Lack of funds, lack of interest on the part of the top management.

xiii. Employee awareness at line and supervisory levels.

xiv. Risk management is viewed as a blocker to a technology-based company—e.g., speed to market, etc.

xv. Getting executive buy-in has been the biggest hurdle, with collaborative efforts at implementation of the strategies a close second.

- **How would you describe the value of a holistic risk management approach to your business?** Most CSOs noted that this approach has been invaluable to their organizations, even calling it a possible business differentiator to customers. Non-CSO responses were largely positive as well, though more respondents saw this initiative as only potentially worthwhile—if numerous challenges could be overcome. Here's a sampling of what both groups encountered.

  a. *Responses from CSOs included:*

i. Very valuable. Firm is very risk-averse; however, risk analysis infuses realistic solutions that make sense for our type of business. When security speaks up, everyone listens as they know how critical it is to the firm's reputation and success.

ii. It is a very valuable tool to recognize the risks each business unit faces and how other units can assist in mitigating or preventing those risks.

iii. Invaluable. Executives today spend half their time growing the business and the other half managing risks.

iv. Business added-value essential to successful anticipation and management of risks, and prioritization of resource and total business effort, as well as improving efficiency and productivity.

v. It's very valuable and basically easy to use, but it requires creating a common language for the terms of the process and also for the metrics of the process.

vi. Avoids duplication of effort; ensures sharing of resources, and helps to establish priorities.

vii. Invaluable. We have a very successful program that would be far less so if the solutions were not first vetted and sometimes negotiated with our business units. We have worked together to create and support a message that the primary purpose of our security efforts is to protect the business, our clients, and by extension, our profitability. It works.

viii. This will allow us to be proactive, reduce risk, and provide a marketable "business differentiator" to our customers.

ix. It is a valuable tool in what we do and how we "sell" our support services.

x. It provides management with a consolidated, ranked view of risk to the organization and enables business cases to be made for projects, budgets, staffing, etc.

b. Responses from non-CSOs included:

i. I think the value is high, but expressing that value to other stakeholders has been challenging.

ii. Highly beneficial in driving business growth.

iii. It helps to have a risk input to the business managers so as to better promote the relationship between business and risk.

iv. Concept is not accepted in Europe as it is in USA.

v. It is very critical because all our businesses are so interdependent they must understand how an interruption in one business affects the others, and/or the possibilities to reduce risk through internal cooperation.

vi. Integral to smooth operations but a long way off.

vii. I consider this to be the latest fad that has yet to prove its worthiness.

viii. Reality contradicts the ability to have a holistic approach.

ix. Gets people to work more closely together since all realize they are stakeholders in the outcome.

x. Embedding ERM in the organization increased our level of risk awareness. This means looking out for potentially harmful new risk exposures; and at the same time, looking for opportunities to add value by responsibly taking on more risk. The value this created has been exceptional.

xi. Important only if CEO sees a benefit in the result (minimize losses, increase profit, minimize risks, increase security).

xii. In my opinion it is a very high-value item, but I believe the general public will not understand the importance until an incident is thwarted by preparation.

- **How did you measure your success?** CSOs offered some examples of how they measure the ROI of these programs. However, not all of them involved typical measurements of metrics, but rather a less tangible but still very important sense of confidence and buy-in from other executives, which often translates into greater funding for security measures. Non-CSO responses often pointed to very precise types of measurements, such as reduced insurance premiums or calculable reductions in loss, but quite often noted that corporate profitability was a sign that the program was working effectively.

a. Responses from CSOs included:

i. Measures include executed plans for addressing the particular risk and calculated risk score-reduction year over year.

ii. Senior voice interchange, level of engagement with client staff, education of security staff.

iii. Improved confidence in the validity of our stated risk exposure. Previously this had been little more than an educated guess.

iv. Still working on proper measurements.

v. ROI measurements, but these have greatest legs in IT.

vi. Measurements based on pre- and post-implementation of countermeasures, controls, personnel or SOPs.

vii. Currently none, are exploring scorecards.

viii. We included the cost-of-loss formulas. By taking actions to reduce the losses we can show success.

ix. Buy-in from senior management, funds released to improve security measures, and creation of new positions at senior levels to ensure continued attention to this issue.

x. Management acceptance and effective management of crisis.

xi. Still measuring! Centralized reporting metrics (incidents, loss, etc.), financial transparency on costs and achieving efficiencies in SRM areas, and feedback from internal and external stakeholders.

xii. Reduction in losses and the overall improvement in the support we receive from the operation divisions.

b. Responses from non-CSOs included:

i. Better decisions on business made. Profitability higher on risk being understood beforehand so right decisions on manning levels, etc., were taken and highlighted to client.

ii. By the relative peaceful atmosphere existing now to allow company activities with little disruptions.

iii. Defined key performance indicators, but mainly reducing the financial cost of risk year to year.

iv. Reduction in insurance premiums and increased scores on third-party risk audit.

v. Six Sigma was one approach, but demonstrating to senior executives through the use of the security risk model that losses could be significantly reduced was the best received.

vi. Civil litigation levels and overall productivity.

vii. Via number of claims, reduction in losses, incidents occurring on campus versus the community we're in.

viii. Operational objectives. Reduction of loss. Increase in profit.

ix. No injuries to employees and members. Reduction in fraud and asset losses and insurance premiums.

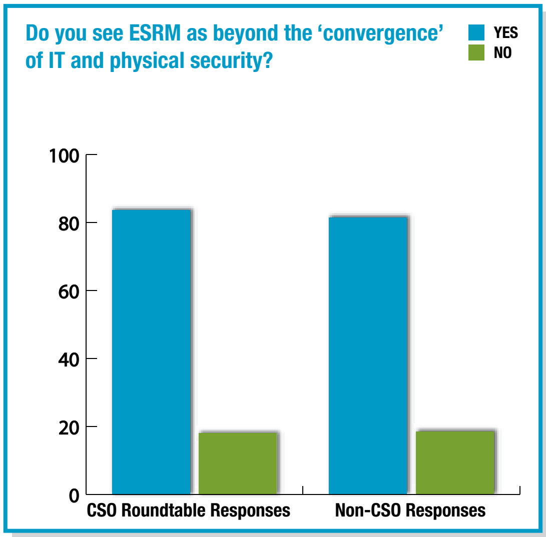
x. Compared to previous performance and calibrated against a best practice.

xi. Profitability of the business as a whole.

xii. Our risk management branch has actuarial-determined savings now approaching a billion dollars.

ESRM: The Big Picture

- **Do you see ESRM as beyond the 'convergence' of IT and physical security? If so, why?** More than eight out of ten CSOs and non-CSOs agreed that ESRM is larger than the convergence of physical and IT security. Here are some of the reasons they believe this is the case.



a. *Responses from CSOs included:*

i. IT and security threats ripple into all aspects of a business, especially along competitive intelligence (CI) lines.

ii. It is more complex and involves risks that go beyond any suggestion of the convergence of IT and physical security.

iii. It is a logical progression from convergence to adopt a holistic view of risks and managing risks in today's interconnected-systems-dominated business environment.

iv. The ESRM paradigm is all-inclusive of other related functions such as environmental health and safety; facilities; etc.

v. ESRM is addressing the totality of risk for the company.

vi. Because specific risks (business continuity, IT disaster recovery, hazards) emanate from a risk management process—they may not align to business objectives unless you conduct that process of evaluation.

vii. Traditional convergence of physical and IT is just one step in the ESRM process.

viii. ESRM involves every business unit in the organization.

ix. Risk is much greater than just the security departments.

x. ESRM should be the philosophy of security's approach in protecting assets.

b. Responses from non-CSOs included:

i. Creates an environment where team members use their individual expertise to achieve a common goal.

ii. ESRM explains the entire relationship between units and necessity of security.

iii. ESRM is a change in culture.

iv. Convergence is far too narrow a concept. ESRM demands a full and detailed integration into corporate processes at every level of operation.

v. IT and physical security are only a small part of what is needed to keep a organization operating during disasters or emergencies.

vi. It's the next step.

- **Do you see an overlap between compliance and security functions in managing enterprise risk? If so, is that overlap increasing?** More than 90 percent of CSOs, and nearly 83 percent of all respondents, said that there is an overlap between compliance and security in managing risk. About 63 percent of CSOs felt this overlap was increasing, while more than two-thirds of non-CSOs said this overlap was increasing.

- **What skill sets must a leader of this type of initiative have?** CSOs mentioned the need for "a holistic understanding of the business" and "knowledge of the company's direction," as well as a deep understanding of "the big picture" of organizational risks. CSOs and non-CSOs alike cited the importance of communication, political and interpersonal skills, as well as leadership and business management. IT savvy was mentioned twice as often as security management by CSOs—indeed, security expertise was not mentioned at all by non-CSO respondents.

- **What groups have the training, education, and networking events that would help security professionals gain the appropriate knowledge and expand their skill sets?** The Risk and Insurance Management Society (RIMS) was mentioned most frequently as the group that could offer appropriate training; a number of academic institutions, including the University of Leicester, the New Jersey Institute of Technology, the University of Kentucky, the University of Denver, and Webster University were mentioned specifically, while many respondents noted generally that they recommend distance education for advanced degrees in business/security management. Forty percent of CSOs pointed to ASIS, with business schools such as Wharton also noted.

Enterprise Security Risk Management: How Great Risks Lead to Great Deeds

If you ask a security executive what his or her greatest concerns are, you won't be surprised to hear that issues such as theft, data loss, and terrorism are at the top of the list. But you might not expect to hear that the economy, competition, and regulatory pressures also rank high.

Security professionals are recognizing that whatever risks their organizations face, they need to reach across all business units to ensure that every department collaborates with the goals of enhancing security, increasing the bottom line, and assisting the organization in meeting its objectives. This is Enterprise Security Risk Management (ESRM). It is a vital element of Enterprise Risk Management (ERM), which examines the universe of risks—financial, strategic, operational, legal, accidental, and so on—that an organization faces.

But where ERM has typically been associated with the financial side of business—such as credit risk and commodities-pricing risk—ESRM highlights the protection of assets and activities such as physical security, investigations, crisis management, business continuity, and data protection. Any disruption in one of these areas could be as harmful to an organization's profit or reputation as a hedge-fund investment or currency-exchange practice. And, unlike a physical security lapse, a bad trade is not likely to put an employee in harm's way.

In October 2009, ASIS International's CSO Roundtable, a membership group of the senior-most security executives from the world's largest organizations, issued a comprehensive ESRM Benchmarking Survey to its members and to the membership of ASIS, asking about the sources of their organizations' greatest risks; the source of organizational support for ESRM initiatives; the business elements included; security's role in ESRM; the department/individual with ultimate responsibility for risk; and various other questions. The survey provided a vital, first-ever benchmark of ESRM across the security industry.

At the same time, the Roundtable interviewed 11 senior security executives from some of the world's largest and most well-respected companies who have first-hand experience in creating and executing ESRM initiatives. These in-depth interviews examined how ESRM projects came about; where support came from; what the challenges were to implementation, and how these were overcome; and what the outcome has been, not only for the organization but for the security professional. The interviews were remarkable in revealing that not only did these organizations end up with better and more efficient ways of assessing and mitigating risk holistically, but the executives found themselves with a vastly increased understanding of and appreciation for how their businesses work that has helped make them successful and respected partners in the C-suite.

Given the sensitive nature of the discussions, the participants requested to remain anonymous. Thus, this paper will refer to companies by business sector rather than by name; however, all the CSOs and CISOs interviewed are either from organizations with more than US$1 billion in gross annual revenue or components of critical infrastructure.

Background of the ESRM Project

Any project that reaches across every unit of a company to define, prioritize, and mitigate risk has to have either very strong backing from senior executives or a powerful security executive pushing the project along.

Backing from the top. Simon, the CSO of a real-estate conglomerate in the Middle East that builds shopping malls, notes that support for his company's ESRM project came from the CEO and CFO, who felt that there were risk management gaps in areas such as fraud, embezzlement, and financial malpractice that needed attention. Steps to close those gaps were made through implementing "a simple but robust ERM program from which security will feature in [managing risk at] properties from design master plan through operation in the shopping mall and the asset management," he says.

Strong C-Suite Support. The ESRM Benchmarking Survey shows that there is significant senior-level support for ESRM projects. Nearly three-quarters of CSOs, and almost 70 percent of non-CSOs, said C-suite support was "strong" or "passionate."

Without the explicit backing of the CEO and CFO, the project would have lagged, he adds. "I think it's critical that they are sponsoring [ESRM]; otherwise I don't think it would move as quickly as it could." Simon, along with the head of IT and the head of finance, reports to the CFO, underlining the close connection of ESRM with traditional ERM.

Petri, the director of enterprise risk and security management of a European company that delivers radio and television services, says that in his case, support from the top was also strong. "The managing director initiated the creation of the risk management process," he says. "She said that she wanted risk management to be the top level, and corporate security would be part of risk management."

> "From the beginning, our goal was to adopt the concept of ERM; that is, to include all risks into our RM process, not only, for example, financial or business risks."

John has created ESRM initiatives for several companies in different sectors, both as an internal CSO and an external consultant. These initiatives "were driven from a very senior, significant level in the organization—boards of directors, audit committees from those boards of directors, and risk committees from those boards of directors." In the case of a utilities company, he says support was strong because the initiative began while both 9-11 and the post-Enron meltdown were fresh memories. "What we were looking at doing was being able to identify both financial credit and operational risk, and roll up to the audit committee and risk committee components of the board."

Support in another sector where John helped spearhead an ESRM initiative was given "solely because board members were sitting on other boards that had implemented ERM, and the board drove the ERM model to the organization," he notes. "They said, 'We want to be able to see and report on this and understand financial credit and operational risk.'"

Fighting for support. But C-suite support is not always there, and so sometimes ESRM needs a strong security executive to simply make it happen. Marene, the CSO of a healthcare company, had to forge a project without strong backing from the C-suite—or anyone else. "We had just implemented the HIPAA (Health Insurance Portability and Accountability Act) security rules that required vendor reviews and the business did not understand the concept. We had to stand up a program and then gain senior-level support—I was fairly new and came in and created the security governance," she says.

Dave, the CSO of a city where Olympic games were held, was able to accomplish the first step of an ESRM project—the convergence of IT and physical security—by making a compelling case to senior management. "I was able to win executive support because we had the Olympics coming," he says. "I said, we've got all this duplication, two reporting chains reporting to senior leadership, risk-based decisions having to be made comparing dollar costs, allocation of different projects whether physical or information or other risk ones, without a good standard or being able to value that risk. I said, if you let me do this I will reduce risk and your costs and I'll need 50 percent less of your time." Senior managers saw an offer they couldn't refuse and took Dave up on his challenge. His ESRM initiative was born.

Some interviewees noted that when top leaders understand risk holistically to begin with, it's possible to have ESRM in place without realizing it. Joe, the CSO of a company that operates data centers and co-location facilities, says, "We didn't know what ESRM stood for but we were doing it. Everything we look at is from a model of risk, so support is phenomenal in our company. It has a lot to do with the type of company we are, since we protect our customers from events."

Stakeholders

Who should be part of an ESRM initiative? The interviewees emphasize that every unit of the organization must be considered. John puts it clearly: "The right people to think about functionally are the owners—that's where you get the risk information from." He mentions physical security, information security, business continuity, and human resources for starters.

"Governance and internal audit ran the project," says Richard, head of group fraud risk and security with a European telecommunications company, "engaging with subsidiary operating companies according to who in the particular operating

Together at the Table. ESRM initiatives bring players together from across the business. The ESRM Benchmarking Survey shows that business continuity planning, IT and IT security, and brand protection were the business partners most often incorporated into the risk management strategy. Brand protection was mentioned by about a quarter of the CSOs, but by few non-CSOs.

company had responsibility for risk management. Other group functions such as legal, external affairs, and security were also involved. Security is an essential partner," Richard says.

Council approach. The various stakeholders in an ESRM effort are often engaged by a risk management group or committee. "Risk management process development was part of the overall process development in our company," Petri says. "I was in charge of it and there were a number of people from different units of the company involved as the Risk Management Process Team. These people changed as the work progressed. From the beginning, our goal was to adopt the concept of ERM; that is, to include all risks into our RM process, not only, for example, financial or business risks."

Rich, senior security director at a global pharmaceutical company, said that his company's efforts toward ESRM began as a result of major counterfeiting operations that targeted the company's products. "The decision was made that a steering committee would be developed consisting of three senior-level executives, and that reporting to this committee would be the working group. The working group consisted of representatives from security, manufacturing, legal, quality assurance, marketing/sales, and public affairs. First course of business was to anoint a leader—that was corporate security," he says, since, given the nature of the brand-protection challenges, security was viewed as the business unit best positioned to facilitate this cross-divisional working group.

Joe says his organization—the hosting firm— has "a unique company structure" that is all-inclusive. During risk management meetings, he says, "Our controller is in the room the whole time, so for us, the insurance aspect is a prerequisite from day one." Also involved in the risk management discussions are representatives from human resources, assurance, operations, and security.

> **"Our initial strategy was to get consensus of what security's responsibilities are and obtain confirmation that our philosophy was consistent with the executive's expectations."**

A higher profile for security. Brian, the CSO of a North American cable and telecommunication company, started by making it clear when he joined the company that security's profile was too low. "I was rocking the boat with the CFO letting him know that we don't have the right alignment—we reported too low in the organization, and we needed influence, and were not properly aligned with the current risk profile of the company. To get to that point, our initial strategy was to get consensus of what security's responsibilities are and obtain confirmation that our philosophy was consistent with the executive's expectations, so we put together the security council," he says. That council comprised the CIO, CFO, the head of human resources, the compliance officer, the controller, and representatives from engineering, legal, internal audit, operations, and customer care.

James, the Europe-based CSO of a multinational pharmaceutical firm, says his company's compliance committee has a key role, endorsed at board level, in assessing and mitigating key threats to the company. "The membership of the committee—which includes people like the CSO, the head of audit, the head of R&D, each of the compliance officers for the major functional areas, the head of information assurance, the head of financial controls, and the corporate responsibility lead—means that it is the ideal forum to enable a holistic approach across the business." It was clear that security was essential to the effort. "It was recognized right up front, that there are risks the company faces that security has a core role in mitigating; in effect, security was drawn into the process as an integral stakeholder, not as an afterthought," he says.

Room at the table. John stresses that composition of any ESRM-related council must remain flexible. "There are groups that may not initially be brought to the table, but because you have a council approach, they end up being brought in. You'll find that every organization is different and every dynamic will change on a weekly, monthly, or quarterly basis depending on where the company's going, and you may have to involve other people along the way."

Including too many delegates can cause difficulties as well. Rich notes, "I think we almost extended the committee too far. It was almost too embracing, and it was quickly recognized that it was becoming unwieldy and the group too big to achieve any realistic business service at its meetings. So some of the people dropped out; that's not to say that their interests weren't represented, but in terms of them having a stakeholder relationship, that was removed. But we thought it was easier to start off broad brush and shrink down."

Rolling Out the ESRM Project

ERM programs were often in place, interviewees note, but despite the all-encompassing name, these programs typically weren't considering all, or even the most important, risks. Crawford says that his company "had a risk management team that was fractured and tended to look at what perhaps—at least in terms of reputation—weren't the biggest risks. It had a focus on health and safety, which of course is a big issue, particularly for a company in the pharmaceutical sector. But it wasn't addressing things that could affect our reputation, such as quality management, counterfeit brand products, bribery, and corruption; it just wasn't taking cognizance of those."

Best of breed. One way to start building an ESRM project is to look first at existing models for enterprise risk management, such as standards from the International Organization for Standardization (ISO) and the Committee of Sponsoring Organizations (COSO). While their focus may not be on traditional security issues per se, they are well respected and established and they generally cover the universe of risk.

Formalized Risk Plans. No matter what it's called, the majority of security professionals say that their organizations have some kind of formalized risk-analysis process that includes the identification and prioritization of risks, and the development of an action plan. The ESRM Benchmarking Survey showed that nearly 90 percent of CSOs and 80 percent of non-CSOs have such a process.

> The risk management team wasn't addressing things that could affect our reputation, such as quality management, counterfeit brand products, bribery, and corruption.

John says that, in one of his ESRM initiatives, his council looked first at existing ERM models and then used elements of those to create the company's own model that was tailored to the business. "It was something that was just starting, and most ERM models were primarily focused on financial risk. Most of the folks who held the CRO [chief risk officer] title at that time were pure financial guys looking at the creditworthiness of the company and the people they were doing business with. To think about things operationally and take it to that level, there weren't a lot of best practices."

"What is not commonly realized is that a number of IT regulatory requirements call for some type of risk management program," Marene, of the U.S.-based healthcare firm, says. "So we leveraged those requirements to implement a formal risk management program where we identify risks and provide a report to the business owners for sign-off."

Define and conquer. Brian, the CSO whose ESRM effort is still underway, says that the first step his group took was to agree on a mission philosophy. "The philosophy is that the security group is there to identify all forms of vulnerabilities and risks in all of our assets, and that could be products, facilities, and reputation. Next, we are prioritizing and understanding risk, whether it's value, regulatory, reputational, and so on. Then, we're establishing remediation plans for those risks (including awareness, training, tools, and insurance). Next we're providing remediation plans to business owners and helping them implement the plans if they want assistance, and if they don't, we make sure that if we are going to accept the risk that the risk is signed off at the appropriate level. Finally, we are responding to incidents as they occur—learning about the vulnerability and coming up with mitigation plans, so once a vulnerability occurs, basically we circle back into assessment mode again. That to me is the fundamental working philosophy of ESRM."

Once that philosophy was agreed to, the real challenge began, Brian says—to differentiate ESRM from ERM. "It's still to be defined how ESRM fits into ERM—is it another component? I don't know. It probably changes by company. But I think the big problem is that it's not defined, and there aren't any [standardized] responsibilities around it," he says.

The lack of definition led to conflicts with the ERM group, Brian says. They complained, "'This is what we do.' My answer was, it's different, here's why, and we got into some of the day-to-day operations on the security side, and I gave them some examples of how we do risk management versus what they do." For example, where identity thieves were stealing company services, the ERM group contended that outstanding money is a collections issue, not a security issue. Brian pointed out to them that "it's not a collections issue if somebody has taken identities three or four times with no propensity to pay. By the time it gets to collections it's not a collections issue anymore, it's fraud."

Brian says the major challenge is defining security risks and ensuring that they are distinct from other risks. "What's the security risk? That part has to be answered. Once you go beyond the scope of that you've gone beyond what your responsibility is. I think that if you can define security risk, you're within the realm of your responsibilities, and that's where you can really have some standing to push back on internal audit or whoever's doing ERM, because they're not doing what we do. So we just need to define and put our arms around it."

Security as advisor. Interviewees stressed that the focus on working across the whole organization meant avoiding having security seen as a naysayer. Instead, they worked to ensure that business managers fully understand the risks they face and then explicitly accept risks if they're not willing to follow security's suggestions.

Security is an advisor to decision makers in the same way that corporate counsel is an advisor, Brian says. "What legal does is provide guidance; they very rarely say 'you have to do this.' They do sometimes when it's regulatory, but most times they say, 'If you do this, this is what's going to happen; if you do that, that's going to happen.'" He says security should provide guidance in the same way and feels that there is very little that security 'owns.' "My recommendation is to do this, but typically it's a business or departmental decision. With the subscriber fraud issue, it's not security's role to make the decision on who our customers should be; however, we should be pointing out the risk, providing analysis, and ensuring that those risks are known and being accepted by the right level of management."

Marene agrees. "If we bring in a new company to outsource some sort of work and they do not have a business continuity plan, we don't make it about them not being allowed to be used because they don't have a business continuity plan, but we make it a risk and then publish a report." Security is using its expertise to identify risks and ensuring that business owners understand these risks, and then suggesting how these risks could be mitigated, but the corporate leadership must decide when to accept these suggestions, and when to reject them.

Technology

Technology is available to help ensure that ESRM efforts are efficient, but finding the way through a maze of options challenged, and continues to challenge, interviewees. The first priority, they say, is to determine what types of data need to be aggregated and analyzed; this also means cultivating a good working relationship with the IT department.

Calling all data. John explains that his search for technology began with understanding what data was most needed. "You have to identify the requirements first and then go find the tool. When you start going through this exercise, you ask, 'What is it from an operational risk perspective that we're looking for?' Then you build the requirements, look at the systems and processes that are in place, and ask, 'Is this an efficient way for us to gather this data?'"

> **Anyone and everyone who comes to the ESRM table will have a set of biases that will need to be understood and addressed. It requires a level of transparency that can be uncomfortable for some.**

"From the tactical level, part of it is your whole case-management system; part of it is your financial reporting tools; and then pulling them all together in terms of a dashboard," John says. "It's a combination of all those elements." In his case, he has found that granular controls on identity- and access-management are critical, and he mentions large players such as Symantec and smaller shops like Quantum Secure. Incident management tools such as those by D3 Security Management Systems and PPM 2000 have helped him to manage physical and information security incidents. All these tools, he says, need to "hook into the bigger aggregators, the dashboard views of the world."

Richard says that his company purchased risk management software tools from Cura, which helps manage governance, risk, opportunity, and compliance across the organization. He adds that some of the operating companies use other risk management tools, or elements of them.

Clearly, the number of products on the market can be daunting, Simon says. "We're keen on examining what's in the marketplace for software that can help us in reporting and managing the risk. There are some good systems out there and we'll probably reexamine those. I deal with all risks, including IT risks, as part of the risk management process, except financial risks such as credit rating, foreign exchange, debts, and capitalization, which goes to Treasury." His organization lost its information security manager when the company restructured, so now Simon collaborates with the head of IT to examine the IT-related risks, including business continuity, system failure, and general information security.

Tool time. Others, like Petri, say they haven't yet moved toward ESRM technologies; and some, like James, would like to but have run into problems along the way. "There were two issues," James explains. "One was integrating it into our current systems, and second was the cost. We felt that in relationship to the cost/benefit ratio, it just wasn't there. So what we did was reduce the number of diverse systems we had as much as we could, simplified them as much as possible, and ensured better integration. Once we have demonstrated to the business the benefits of simple, lean, and agile processes and technology, we anticipate increased willingness to invest for the long term."

Those challenges are ultimately for the best, he says, since they force him to consider more deeply what's needed. "There's people and process," James says. "Let's address the processes and see if we've got those right, then let's address the people issues. Then having looked at the two of those, let's see if there's any technology that's going to support those. We're not there yet. We find the people, simplify the processes, and eventually invest in the technology."

Specific Challenges

Dick, the CSO of a multinational biomedical research firm, says, “Once implemented, a successful ESRM program is one in which the business risk considerations are viewed holistically. This is sometimes harder than it sounds because the participants in the process have to shed their personal agendas for the sake of the greater good. Anyone and everyone who comes to the ESRM table will have a set of biases that will need to be understood and addressed. If handled properly, there can be a great deal of information gleaned from this exercise. But it requires a level of transparency that can be uncomfortable for some.”

Business first. Marene points out that many challenges arise because security professionals don’t “pull off the security mask and put on the business mask, and look at risk from the eyes of a business professional.” Since she’s in an industry that processes credit cards, she gives an example of a business-unit owner asking what the implication would be if the unit wasn’t compliant with payment-card industry specifications. Marene’s answer: “You have options: you can secure the data, you can remove all the data from the files and implement a process to stop retaining it, you can agree to pay the fines, or you can stop processing credit cards.” The business owner quickly understood. “He wasn’t going to do anything until I put it in business terms and said, ‘Make a choice.’ It’s so hard for security professionals not to say ‘you have to secure it.’” The business owner must decide to eliminate the data and change his business process.

Obstacles Along the Way. Funding, personnel, and support were the obstacles most frequently mentioned by CSOs and non-CSOs alike in the ESRM Benchmarking Survey. But other concerns were raised as well, such as a lack of support from staffers when the information created by a risk committee is labeled ‘confidential’; finding time among limited and competing resources; and the conception that risk management hinders technology-based companies.

> **“You have to explain to people that this is a partnership for the betterment of the organization, and it has nothing to do with a hostile takeover or finding some inefficiency for audits.”**

Overcoming fears. John says that while skills and dollars are always near the top of the list of challenges, his experience shows that fear and misunderstanding have the potential to break the whole process. “People are concerned. They don’t like change; when someone starts dipping into their functional area and starts asking questions, people get nervous. You have to explain to them that this is a partnership for the betterment of the organization, and it has nothing to do with finding inefficiency for audits, or a hostile takeover, which is the first thing to come to people’s minds.”

Simon agrees that employee concerns are a major source of pushback. “ESRM will improve processes and efficiencies, and therefore people are worried about their jobs,” he says. “It’s like the business continuity story, where if you ask someone what’s critical, everything’s critical; if they say they’re not critical they believe they haven’t got a job. But it’s not like that, it’s being a bit more mature.”

Silo busting. “For us it was centralization versus decentralization,” James says, describing the concern ushered in by the adoption of ESRM. He explains that his company is very decentralized, and ESRM has shaken up peoples’ perspectives. “In the pharmaceutical sector you’ve got so many cultures within the organization: research and development, sales and marketing, operations; each has its own idea of ‘how we do things here,’ and traditionally they’ve operated entirely independently of each other. Now we’re being brought around the table and told that things are going to move from the extremes of the decentralization/centralization spectrum towards the middle. That has a lot of implications for how you operate across cultures, across those silos we’ve been operating in all those years. So it’s certainly brought out a lot of interesting discussions.”

Those “interesting discussions” have also been, at times, acrimonious. “Some people frankly were really miffed; to encourage change it meant that a stake had to be put in the ground: if people did not want to buy into the changes then they had to relinquish their role on the committee. Fortunately, this was a very small minority.” Brian, of the cable company, says that he ran into some turf wars with internal audit and IT that were pacified when he explained the ESRM philosophy. “If the CIO says, ‘You don’t know about technology,’ you say, That’s right, but I know about risk and, I’ll tell you that your IT folks probably don’t know as much about regulatory risk as I do, or liability, because these are my skill sets. If there’s a potential data breach, who is more equipped to do that investigation? IT or someone with a history and background of being able to interview individuals, or who has the resources to track down missing tape or engage law enforcement resources?”

Simon says that the understanding of the importance of a holistic view of risk is growing. “What I’m excited about is that I see a lot of people waking up to it because they’ve seen what can happen if you don’t do it. The financial crisis was a good example. I don’t think people have understood it sufficiently to buy into it, it takes a lot of education, but now people are starting to understand and the rationale is much clearer.”

Outcome of an ESRM Initiative

ESRM is meant to provide a holistic view of security and enhance an organization’s ability to identify and mitigate risks. But those interviewed say they saw a host of benefits from their rollouts that they hadn’t expected.

Business chops. “I learned more about the way business was run and how the thought leaders in various business units operated,” Rich, in pharmaceuticals, says. “It was a wonderful opportunity to see how things get done in another part of a company on a routine basis. It gave me the opportunity to know what and how they’re thinking, and I could take that experience and apply it to the rest of my career and short term as well.”

A Measure of Success.
Metrics are key to assessing the success of an ESRM program, but according to the ESRM Benchmarking Survey, there are as many soft metrics as hard ones. CSOs pointed to the importance of confidence and buy-in from other executives, which often translates into greater funding for security measures. Non-CSOs mentioned measurements such as reduced insurance premiums or calculable reductions in loss, but also noted that corporate profitability was a sign that the program was working effectively.

> **Leading the risk management effort is about being supportive to the business objectives and the board's goals.**

"The outcome is that you become much more intelligent about your business and your vulnerabilities," John says, "and because you're becoming intelligent and you have that visibility and you're not relying on FUD—fear, uncertainty, doubt—to try to get funding, you can go to the board, management committee, or even the CEO directly, and say, 'We've been tracking this on a weekly/monthly/quarterly basis, you can see where we have exposure.' Then you put a business plan together to mitigate that exposure. That's where the tools become helpful. But the reality is that it can be frustrating. You may see an intolerable risk, and the executives of the company say, 'We're going to take that risk, our appetite is there.'"

Says James, "Everybody is much more clear and focused on what they need to achieve. I think as well it's brought more positivity; whereas before people may not have been entirely convinced and would do things simply because they had been asked to do it. At least now people feel that they have a say, they can influence how it is delivered, recognize the bigger picture and see where the priorities must lie. "The ERM process development and implementation has increased the knowledge of risk and its management throughout the organization," says Petri, of the European TV/radio firm. "It has helped to create a common language and vocabulary, which is necessary."

Education and awareness. According to Simon, "I look at security guys, for many of them their comfort zones are in security programs and strategies. They are all very good and some are much better security managers than I'll ever be, but [their expertise] isn't in terms of the risk management framework which business understands. I think that's the key for us: we're trying to educate people globally where you can get benefit from security risk management."

Brian notes that going through this process has made it clear to him that in his organization "we have done a very poor job in security awareness. We do a good job when we do it, but we haven't accepted that security awareness is a daily part of our responsibilities. It should be. Every time I get frustrated over why corporate executives don't get it, it's because we haven't made them aware of what we do. Every time we do make them aware of our philosophy and our approach, there's an acceptance of it."

He plans on setting up meetings each month with different departments and discussing their specific security issues. "As you do that with each of the different pieces, they get much more of an understanding of when they should get something to security. It's a cultural mindset to change."

The Necessary Skill Sets

To be a successful ESRM leader, a wide range of skill sets is required. According to interviewees, these skills are less related to security knowledge than they are to business savvy.

Supporter and leader. “Leading the risk management effort is about being supportive to the business objectives and the board’s goals, and aligning yourself with those and pushing the program as part of the board’s overall business aims and objectives,” says Simon. “To understand the business, you don’t have to be a CFO or developer or retailer; what you have to be is a very good generalist and a good leader, somebody who is able to make decisions and get people of different functions and organizations engaged.”

“What I’m able to provide is change management,” Simon adds. “The implementation of a program involves change, and if you’ve got a skill set that includes understanding business processes and understanding the business, as you would if you were a consultant coming in to examine process flows and working relationships, that skill set helps with a risk management program.”

Just as important is knowing who to go to for help, he says. “I have people in finance I can call on for that skill set; I’ve worked closely with IT and IT development, so if I have any knowledge gap in terms of skill sets with IT infrastructure and technical details, I’ve got people within the organization that I work with whom I can call on.”

What You Need to Succeed.
A lot of skills are important for leading ESRM initiatives—from “a holistic understanding of the business” and “knowledge of the company’s direction” to a deep understanding of “the big picture” of organizational risks. In the ESRM Benchmarking Survey, CSOs mentioned IT savvy twice as often as security management skills—and security expertise was not mentioned at all by non-CSO security professionals.

According to Richard, the telecom CSO, what’s most important is “a wider understanding of what is driving—and therefore what can influence—the business beyond security and malicious threat concerns.”

Communication skills. “It’s really about your personal ability to communicate, understand how others communicate. I’m not sure that’s something that is a learned behavior but I think it can be developed,” says John. The first skill is to be able to get past the initial mistrust. “It’s fostering those relationships and letting those people know it’s not us coming in and taking your headcount, but the ability to articulate that this process is for the betterment of the organization. It’s not about building my organization or ‘convergence’ in the sense that we’re going to put two departments together—it’s your ability to communicate well and come off with that soft approach.”

Petri says the key skill is the “ability to ‘talk business.’ To put it shortly I’d say any and all skills that help the CSO to communicate throughout the organization, with every business unit, with every employee.”

> “The reality is that it can be frustrating. You may see an intolerable risk, and the executives of the company say, ‘We’re going to take that risk, our appetite is there.’”

Brian says that his background as an attorney has given him invaluable insights into the business risks and therefore how to implement ESRM. “Any time you can learn about liability, via continuing legal education, that’s helpful. Not because you want to talk like a lawyer but because it makes sense as to why we do things. The main drivers for security are that you have potential liability, regulatory requirements, or you had an incident fresh in people’s minds, which come and go.”

Common sense. Marene argues that general business skills aren’t always enough. “I’ve seen plenty of people with business backgrounds who have no sense of adapting to the organizational culture. When you work in a corporation, it’s learning how an organization works. Every corporation has a different culture, and you have to know how to work in your corporate culture.” Otherwise, she says, no matter how good your ideas are, they’ll fall on deaf ears.

Moving Ahead with ESRM

ESRM initiatives are clearly not simple or fast to roll out—one CSO noted that it took 18 months in one case just to get the initial framework set up. They require strong support from top managers, or a commanding advocate in the CSO’s chair, someone who has the ear of top executives. Corporate-wide councils need to be chosen with care to ensure that all risk areas are included and fairly prioritized. And each step of the process brings the potential for conflict with other business units.

The rewards are well worth it. For the business, it means ensuring that a much wider range of risks—including many that ERM efforts don’t fully consider, such as reputation, brand, and physical risks—are considered with an expert eye. For the security professional, it means developing a better understanding of the business that can significantly enhance a career.

Sitting on the sidelines will mean missing the chance to play in the game, however. One CSO said he is watching security lose the agenda and getting stuck responding to internal audit or other traditional ERM functional areas. As these security leaders noted again and again during interviews, it’s not enough for security professionals to simply bring their extensive expertise to the table; even top-notch business skills aren’t enough. Only once security executives understand how ESRM works and how it can help not only mitigate risks to save money, but also take advantage of opportunities and make money, will they be given—and have fully earned—their place at the corporate table.

ASIS
INTERNATIONAL
Advancing Security Worldwide®

About ASIS International

ASIS International (ASIS) is the preeminent organization for security professionals, with more than 37,000 members worldwide. Founded in 1955, ASIS is dedicated to increasing the effectiveness and productivity of security professionals by developing educational programs and materials that address broad security interests, such as the ASIS Annual Seminar and Exhibits, as well as specific security topics. ASIS also advocates the role and value of the security management profession to business, the media, government entities, and the public. By providing members and the security community with access to a full range of programs and services, and by publishing the industry's number one magazine—*Security Management*—ASIS leads the way for advanced and improved security performance. For more information, *visit www.asisonline.org.*

ASIS INTERNATIONAL

CSO ROUNDTABLE™

The CSO Roundtable provides a dedicated forum for the most senior security professionals from the largest and most influential organizations in the world. An initiative of ASIS International, the CSO Roundtable became its own membership organization in 2008 to gain recognition for and enhance the standing of the CSO position; to assist CSOs in job performance, leadership and professional development; and to develop the next generation of corporate CSOs. For details, visit *www.csoroundtable.org*.

ASIS INTERNATIONAL
Advancing Security Worldwide®

1625 Prince Street
Alexandria, VA 22314-2818
USA
+1.703.519.6200
Fax: +1.703.519.6299
www.asisonline.org