BY MICHAEL P. JOHNSON
& JEFF M. SPIVEY

ERM

AND THE SECURITY PROFESSION

Many organizations are competing to provide the definition of enterprise risk management. Each definition is written from a different vantage point and paradigm, with each attempting to promote a more contemporary process model toward an enterprisewide, holistic view of risk management aligned more closely with business processes, organizational goals and objectives.

The security profession has been struggling to develop methods that align selection criteria for physical and logical mitigation controls with the fundamental aspects of risk management and organizational goals and objectives to quantify returns on investments in security people, processes and technologies. Security and risk management professionals continue to struggle with the inability to quantify a nonevent. How many times in our careers have we experienced the frustration of senior management's decision to reduce funding in our respective areas of responsibility because nothing happened? Is the absence of incidents the result of effective security and risk management? Or is it the absence of risk itself?

Numerous factors inclusive of regulatory and marketplace drivers have provided the means to answer these questions and many more. Among these factors are:

- the evolution of the concept of security convergence—the combined management of physical and logical security along with risk management and business continuity—into the framework of enterprise security risk management (ESRM) establishing and representing the function of security as a component of a comprehensive ERM model
- the enactment of new federal regulations for the creation of certified security management systems providing the opportunity for specific tort liability reduction in the event of a terrorist attack, a potential reduction of insurance premiums and the potential reduction of underwriting losses.

- the recognition, acceptance and adaptation of the practices and principles of guidelines, standards and frameworks propagated by entities like the International Organization for Standardization (ISO), ASIS International, the National Fire Protection Agency (NFPA) and the U.S. Department of Homeland Security (DHS).

Herein is a synopsis of the factors that enable security and risk management professionals to collaborate and quantify the effects of their efforts on the organization's bottom line.

From Security Convergence to ESRM

ASIS International, the world's largest organization for security professionals, is playing a major role in the refinement of a new security paradigm in the backdrop of risk management; paving the way for a natural migration and progression from security convergence to ESRM.

The first major initiative was the co-creation of the Alliance for Enterprise Security Risk Management (AESRM) in February 2005. This organization embodied the collaborative efforts of ASIS International, the Information Systems Auditing and Control Association (ISACA) and the Information Systems Security Association (ISSA) to accelerate the understanding and adoption of convergence between physical and logical security along with the long-term goal of developing approaches for enterprise security risk management.

According to the AESRM, "The need for the alliance is predicated on the significant increase and complexity of security-related risks to international commerce from terrorism, cyber-attacks, Internet viruses, theft, fraud, extortion and other threats that require corporations to develop a more comprehensive approach to protect the enterprise. That approach often features convergence, a holistic view of security that takes an integrated approach to information and traditional security. It ensures that all functions within the enterprise work together to identify and mitigate risks, and to effectively manage security-related incidents to reduce a potential negative impact on people, profitability and property."

The alliance has four main objectives, which it plans to advance through research, executive seminars and other educational offerings to benefit security and other business executives:

- Develop adaptive risk models that embody interdisciplinary, enterprise wide security risks
- Increase understanding among executive management concerning the critical importance of enterprise security risk management
- Promote consistent enterprise security risk management positions to influence policymakers
- Contribute to the qualifications and competencies of senior executives responsible for security risk.

Security convergence is a powerful concept whose acceptance and adaptation has not moved as quickly as anticipated. Perhaps this is because the word "convergence" has become overused or synonymous with the worlds of technology convergence or regulatory convergence? Or could there be a tendency for most organizations to manage the disciplines inherent in this convergence concept at the tactical and operational levels with little regards to the strategic value of security convergence?

The concepts implicit within ERM address management activities at the tactical, operational and strategic levels, with the lexicon of ERM becoming more prevalent at the C-level suite of corporate officers, regulators, stockholders and financial ratings agencies. The formal integration of the security convergence thought process into an ERM model or framework would work to improve the risk identification, assessment and mitigation activities within any organizational risk management program. This type of an integrated framework raises awareness among executive level managers of the functions and responsibility of security and risk management professionals and their contributions to the sustainable success of their organization.

A new framework called ESRM represents the natural progression of security convergence and a direct link to ERM. The ESRM model does not look to compete with, nor replace, traditional ERM definitions or models, but represents an opportunity to clarify security's role in risk management while following ERM's cross-functional collaboration with a broad range of disciplines.

ESRM REPRESENTS THE NATURAL PROGRESSION OF SECURITY CONVERGENCE AND A DIRECT LINK TO ERM.

Enterprise Security Risk Management

In order to facilitate migration beyond security convergence toward the more holistic model of ERM, the following is a proposed definition of ESRM:

"The component of an enterprise risk management model focused on the security perspective for identification, assessment, and mitigation of those events that impact an organization's ability to achieve its business goals and objectives, ESRM concentrates on organizational activities relating to the planning, prevention, response,

resiliency, recovery and resumption of events; creating physical, technical and administrative mitigation controls that provide for the deterrence, detection, assessment and response to such events. ESRM is a holistic risk management process that aligns organizational drivers affecting strategy, processes, people, technology and knowledge to protect key assets in accordance with governance, risk, and compliance (GRC) requirements. ESRM requires cross-functional collaboration within the back drop of ERM between multiple management disciplines including, but not limited to physical and logical security, safety, legal, risk management, crisis management and business continuity planning."

ESRM demands that security organizations develop a holistic view and understanding of all risks that could potentially affect the enterprise. Security must also understand its roles and shared responsibilities in managing all risks. The traditional silo approach to risk management is replaced with a new paradigm in which everybody must understand and share the responsibilities for the coordinated management and treatment of risks.

The broad acceptance of this definition of ESRM—or one like it—will provide the missing link between security, security convergence and ERM. This definition does not aspire to compete with or replace existing ERM definitions, frameworks and methodologies. Quite to the contrary, ESRM in accordance with definition above is designed to be a "component of an ERM facilitating cross-functional collaboration between multiple management disciplines."

Security and risk management professionals, auditors, and attorneys do not run organizations, but are normally engaged as advisors to senior management. Therefore it is important that subsequent definitions relating to components of ERM be grounded in the professional discipline and paradigm of the authoritative agency, but be conveyed in a fashion that is meaningful to our collective clients—general business practitioners that comprise senior management of organizations that hire us as advisors. Well-defined, function-specific components of a unifying ERM model, aggregated into a mature ERM framework will strengthen our collective ability to manage risk and safeguard organizational assets.

Federal Legislation Creates Opportunity

The second major initiative of ASIS International is obtaining designation as "certified technologies" for ASIS International Guidelines and professional certifications by the U.S. Department of Homeland Security (DHS) under the SAFETY Act of 2002 providing tort liability reduction in the event of a terrorist attack.

Two recently enacted federal regulations provide for a plan by which approved technologies, processes, methodologies and professional certification used in protection strategies for organizational assets can be certified by DHS, thereby providing varying levels of tort liability reduction.

In accordance with the Support Anti-Terrorism by Fostering Effective Technologies Act of 2002 (SAFETY Act of 2002), U.S. Department of Homeland Security has designated several guidelines (methodologies) developed by ASIS International, and the ASIS professional certification (Certified Protection Professional or CPP) as qualified technologies under this act. The most significant development associated with this approval is that ASIS guidelines providing methodologies that could reduce the risks or effects of terrorism are now qualified as a "technology." This development is significant in that companies can reduce or limit their liability arising out of terrorist acts by using DHS designated ASIS methodologies or ASIS professional certifications (CPP, PSP, PCI).

There is both a "designation" and "certification" under the SAFETY Act. Designation allows for the "seller," or provider of the technology, to be liable for a percentage of economic damages proportionate to their responsibility for the harm with a bar on punitive damages and prejudgment interest. It also provides for the reduction of the plaintiff's recovery by amounts the plaintiff received from "collateral sources" (i.e., insurance benefits) and that claims can only be made in federal court. The cap of damages is set by DHS.

The DHS certification of sellers (providers of the technologies) additionally receives a presumption of immediate dismissal. In *both* circumstances, however, claims against customers are to be immediately dismissed. This opportunity to lower or eliminate liability is significant and should be explored by everyone having terrorism insurance or that believes they may be involved in a terrorist event.

The SAFETY Act only applies to acts of terrorism, not ordinary crime; does not distinguish between a U.S. or foreign entity; and applies to acts of terrorism outside of the United States as well. For comparison, the original

ESRM DEMANDS THAT SECURITY ORGANIZATIONS DEVELOP A HOLISTIC VIEW OF ALL RISKS THAT COULD POTENTIALLY AFFECT THE ENTERPRISE.

Terrorism Risk Insurance Act legislation and its first extension only covered foreign terrorist events. The SAFETY Act covers both foreign and domestic terrorism events (as declared by the head of the DHS) and terrorist events affecting the overseas interests of U.S.-based companies.

The opportunity to understand these risks and reduce liability for the sake of lowering the company's exposure is one important reason to further examine this opportunity. The other reason, which may also be the impetus for immediate action is the possibility of lower insurance premiums related to terrorism. Everyone wins through reduced risks and lower insurance premiums for insured and corresponding lower underwriting losses and higher underwriting profits for insurers.

Risk management considerations are playing an ever-increasing role in security-related strategies and decision-making processes. This development results in an unparalleled opportunity to understand security risks and quantify opportunities for savings. It creates the ability to obtain more appropriately priced insurance resulting in leveraging the upside of risks via a more focused balance of risks and rewards. Not only is the size of risks getting larger, but the convolution of managing them is as well.

Early adopters of the SAFETY Act have used this designation or direct DHS certification in negotiations with their terrorism insurance provider to obtain favorable rates. Whether property owners, property management companies or businesses directly inclined to purchase terrorism insurance, the SAFETY Act can have significant added value and act as a positive differentiator. The ability to understand the upside of the SAFETY Act designation or certification tools can set your company apart when managing insurance costs or demonstrating tort liability reduction for your customers. The upside is measurable and can make a positive and quantifiable contribution to profitability while improving the state of security.

Comparing Notes

Today's regulatory landscape and numerous marketplace drivers have provided the means to quantify the effectiveness and efficiency of investments in security and risk management programs and the security and the risk management professions are beginning to understand the synergies of these efforts. Risk managers have much to share with security professionals regarding risk models, qualitative formulas to measure risk, return-on-investments in risk management and security.

Conversely, security executives can assist risk professionals in the areas of risk identification and assessment providing guidance and prioritization of technical and natural hazards most likely to affect their organization. Additionally, the security industry's focus, knowledge and experience with mitigation controls can be leveraged by risk managers to obtain a reasonable level of assurance about the effectiveness of these controls.

At the end of the day, it is all about articulating the business case to stakeholders and C-level decision makers, enabling them to manage uncertainties as the enterprise creates value. Security and risk managers using the ESRM framework and SAFETY Act designated and certified technologies will be empowered to do good for themselves, their customers, employers and owners. ■

***Michael P. Johnson**, MBA, MSIA, CISSP, HISP, ISO 27001 Auditor, is a founding principal of Security GRC, LLC, a professional services organization that assists clients in building certified security management systems.*

***Jeff M. Spivey**, CPP, PSP, is a vice president for risk intelligence company Risk IQ and a director of security consulting firm Security Risk Management, Inc.*

RISK MANAGEMENT®
A PUBLICATION OF THE RISK AND INSURANCE MANAGEMENT SOCIETY, INC.
MAGAZINE

Reprinted with permission from *Risk Management Magazine*, January 2008 issue, pages 30-35. Copyright 2008 Risk and Insurance Management Society, Inc. All Rights Reserved. *www.rmmag.com*