The Convergence of Physical and Information Security in the Context of Enterprise Risk Management

The Alliance for Enterprise Security Risk Management℠

Deloitte.

The Convergence of Physical and Information Security in the Context of Enterprise Risk Management

The Alliance for Enterprise Security Risk Management℠

Deloitte.

The Alliance for Enterprise Security Risk Management™ (AESRM™, *www.aesrm.org*) is a partnership of two leading international security organizations, formed to address issues surrounding the convergence of traditional and logical security.

About ASIS

ASIS International (*www.asisonline.org*) is the preeminent organization for security professionals, with more than 34,000 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 member 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.

About ISACA

With more than 65,000 members in more than 140 countries, ISACA (*www.isaca.org*) is a recognized worldwide leader in IT governance, control, security and assurance. Founded in 1967, ISACA sponsors international conferences, publishes the *Information Systems Control Journal*®, develops international information systems auditing and control standards, and administers the globally respected Certified Information Systems Auditor™ (CISA®) designation, earned by more than 50,000 professionals since inception, and the Certified Information Security Manager® (CISM®) designation, a groundbreaking credential earned by 6,500 professionals since it was established in 2002.

Disclaimer

The Alliance for Enterprise Security Risk Management (AESRM), *www.aesrm.org*, (the "Owner"), has designed and created this publication, titled *The Convergence of Physical and Information Security in the Context of Enterprise Risk Management* (the "Work"), primarily as an educational resource for security professionals. The Owner makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of all proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, security professionals should apply their own professional judgment to the specific circumstances presented by the particular systems or information technology environment.

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu, a Swiss Verein, its member firms, and their respective subsidiaries and affiliates. Deloitte Touche Tohmatsu is an organization of member firms around the world devoted to excellence in providing professional services and advice, focused on client service through a global strategy executed locally in nearly 140 countries. With access to the deep intellectual capital of approximately 150,000 people worldwide, Deloitte delivers services in four professional areas—audit, tax, consulting and financial advisory services—and serves more than 80 percent of the world's largest companies, as well as large national enterprises, public institutions, locally important clients and successful, fast-growing global companies. Services are not provided by the Deloitte Touche Tohmatsu Verein, and, for regulatory and other reasons, certain member firms do not provide services in all four professional areas.

As a Swiss Verein (association), neither Deloitte Touche Tohmatsu nor any of its member firms has any liability for each other's acts or omissions. Each of the member firms is a separate and independent legal entity operating under the names "Deloitte," "Deloitte & Touche," "Deloitte Touche Tohmatsu" or other related names.

Disclosure

AESRM Member Organizations

ASIS International
1625 Prince Street
Alexandria, VA 22314 USA
Phone: +1.703.519.6200
Fax: +1.703.519.1501

ISACA

3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
Phone: +1.847.253.1545
Fax: +1.847.253.1443
E-mail: *research@isaca.org*
Web site: *www.isaca.org*

The Convergence of Physical and Information Security in the Context of Enterprise Risk Management
Printed in the United States of America

Acknowledgments

From the Publisher

AESRM wishes to recognize:

Primary Researcher and Author

Rick Funston, Principal, Deloitte & Touche LLP, USA
Robert Lane Kimbrough, Manager, Deloitte & Touche LLP, USA
Marc MacKinnon, Senior Manager, CISSP, Deloitte & Touche LLP, Canada
Adel Melek, Partner, CISA, CISM, CISSP, CPA, Deloitte & Touche LLP, Canada

Project Contributors

Leon Bloom, Partner, CISA, Deloitte & Touche, Canada
Glen Bruce, Senior Manager, CISA, CISM, CISSP, Deloitte & Touche LLP, Canada
Christine Bryan, Consultant, Deloitte & Touche LLP, Canada
Ross Couldrey, Consultant, Deloitte & Touche LLP, Canada
Nick Galletto, Partner, CISM, CISSP, Deloitte & Touche LLP, Canada
Mark Layton, Partner, Deloitte & Touche LLP, USA
Chris Lee, Partner, Deloitte & Touche LLP, USA
Sameer Mehta, Deloitte & Touche LLP, Canada
Simon X. Owen, Partner, Deloitte & Touche LLP, UK

Subject Matter Expert Project Contributors

Ken Biery Jr., CISM, CISSP, CPP, CWSP, G7799, Unisys Corporation, USA
Bill Boni, CISM, Motorola, USA
Jonathan P. Clemens, CISM, CISSP, Intel Information Risk & Security, USA
Tom M. Conley, CISM CFE, CPP, The Conley Group Inc., USA
Dave Cullinane, CISSP, CPP, eBay, USA
Marios Damianides, CISA, CISM, CPA, CA, Ernst & Young LLP, USA
Roger S. Dixon, CISM, CISSP, CPP, SCR Consulting Services LLC, USA
Anne T. Ferraro, CISA, CISM, CBCP, CQA, JP Morgan Chase & Company, USA
Steve Hunt, CISSP, CPP, 4A International LLC, USA
Henry (Hank) M. Kluepfel, CISM, CPP, SMIEEE, Science Applications International Corporation (SAIC), USA
Dave Morrow, CISM, EDS, USA
Ray O'Hara, CPP, Vance International, USA
Dick Parry, CISM, CPP, Novartis Institutes for Biomedical Research Inc., USA
John Petruzzi, CISM, CPP, Simon Property Group, USA
Joe Popinski, CISM, CFE, CISSP, CPP, IE, a Dynetics Company, USA
Harry D. Raduege, Jr., Deloitte Center for Network Innovation, USA
Ty L. Richmond, CFE, CPP, Andrews International, USA
Jim Shames, CPP, 5D Pro Solutions LLC, USA
Jeff Spivey, CPP, Security Risk Management Inc., USA
D.A. (David) Stolovitch, CISM, CD, CISSP, CPP, Sun Life Financial, Canada
Dave Tyson, CISSP, CPP, City of Vancouver, BC, Canada
Guido Wagner, SAP, Germany
Timothy Williams, CFA, CPP, Caterpillar, USA
Rick Withers, CISM, CHS-III, CPP, TRC, USA

Methodology and Data Analysis

Olivier Curet, Deloitte & Touche LLP, USA
Cynthia O'Brien, Deloitte & Touche LLP, USA

Table of Contents

Foreword

The convergence of physical and information security might be likened to the early days of flight. While there have been some ambitious attempts at convergence by daredevil visionaries, as described in the case studies, progress, for the most part, has been slow and difficult. The truth remains that convergence, which is typically based on the vision of specific individuals rather than on a structured, well thought-out, repeatable model guided by a clear vision and road map, is still in its early stages.

This is not to demean the convergence progress made to date. Every new idea, by necessity, goes through a cycle that includes trial and error, often ridiculed by naysayers and resisted by those who do not want to let go of the more familiar and comfortable way of doing things. For the visionaries of our case studies, there are some "easy" convergence wins in terms of efficiencies of scale gained by integrating information and physical security monitoring and video surveillance systems on a common organization network. But these advantages cater to technical people and are promoted by the security technology and communications companies of the world. The "hard" convergence wins—the ones that will provide the largest benefit—require buy-in from senior executives. As it stands today, senior management typically sees security more as a tactical function than a necessary component of business processes or decision making.

There are those who see senior management's inability to recognize the importance of security as a lack of foresight. But it is a human truth that, before major change can be achieved, there needs to be sufficient and compelling motivation. How security is perceived may also be an obstacle to convergence. At present, physical and information security are viewed as separate functions with major differences.

There is little doubt that perceptions will have to change before the convergence of physical and information security functions becomes an accepted way of managing security risk. Convergence is intuitive and logical—but it has not yet arrived.

We hope you find this report a worthwhile read. It contains case summaries of organizations that have adopted some model of the converged physical and information security. It also features quotes from those in the industry, giving their views on the outcome and imminence of convergence. Overall, we have attempted to present an objective and realistic view of the state of physical and logical convergence in the security and risk management arena.

Adel Melek
Partner, Global Leader
Security & Privacy Services
Deloitte & Touche LLP, Canada

Ray O'Hara
Chairman, AESRM
Senior Vice President
Vance International

1. Introduction

Background

Deloitte & Touche LLP in Canada was commissioned by The Alliance for Enterprise Security Risk Management (AESRM) to research and develop a report addressing the:
- Value of security as part of enterprise risk management (ERM)
- Benefit of a converged view of security in managing enterprise risk

The material that forms the basis of this study includes surveys and interviews conducted by Deloitte Touche Tohmatsu member firms (hereafter referred to as Deloitte) for AESRM, material developed by Deloitte, and prior research conducted by AESRM.

The survey conducted by Deloitte drew on the insights and experiences of security executives representing traditional and information security disciplines who are members of ASIS International and ISACA, two of the founding members of the AESRM. These security executives provided insight into the:
- General state of security convergence
- Integration of converged security as part of ERM
- Role of risk councils
- Benefit that a strategy for converged risk management plays in breaking down communications barriers between security disciplines and in promoting better risk management among those responsible for managing risk across the enterprise

What Is Meant by Security Convergence and ERM

When the authors talk about converged security in this publication, particularly as it relates to enterprise risk, they are talking about not only physical and information security, but also the wider areas of protection, including security responsibility found within human resources and crisis management as well as within businesses or operational lines of responsibility.

Within the security arena, convergence has been defined as "... a trend affecting global enterprises that involves the identification of security risks and interdependencies between business functions and processes within the enterprise and the development of managed business process solutions to address those risks and interdependencies."[1] This definition addresses the need to break down organizational barriers and obstacles to information sharing that prevent organizations from effectively identifying and managing security risk within the wider perspective of the enterprise.

[1] The Alliance for Enterprise Security Risk Management, *Convergence of Enterprise Security Organizations, 2005.*

Arriving at an acceptable definition of ERM is not easy. ERM remains an emerging concept with a wide range of interpretations that largely depend on the implications of risk in different industry sectors. However, a broad, generic definition of ERM might be that it is a process to manage risk as it affects not only existing assets but also future growth, and to manage that risk from an enterprisewide view. ERM differs from traditional approaches that manage risk in silos and typically focus on risk only as it affects existing assets.

It is hoped that this report will aid organizations in understanding the need for, and the benefit that can result from, taking a wider perspective on risk and gaining an appreciation for the contribution that security professionals provide as part of ERM.

A Shift in Traditional Thinking

A 2005 AESRM report titled *Security Convergence: Current Corporate Practices and Future Trends* concluded that the convergence of security functions is "driving a shift in emphasis on capabilities under traditional operating layers" toward attributes aligned with ERM. At each level, from people through process and strategy, a shift in thinking and operating has been detected, which moves risk management from a functional, technical orientation toward a business-based, adaptive approach to risk management. This shift requires a common vocabulary and unifying approach that come together at the executive and board levels as part of an organizational strategy.

Figure 1 illustrates the shifts in emphasis across people, processes and strategy.

Figure 1—Shifts in Thinking: People, Processes and Strategy

	Operating Levers	FROM	TO
Strategy	Risk Management	Asset-based view	Enterprisewide view
	Governance	Passive and infrequent	Active board involvement
Processes	Budget Processes	"Not my domain"	Common language with peers
	Standards and Guidelines	Functionally focused	Common and shared widely
	Integration	Forced	Adaptive
	Business Case	Technical/jargon-filled or none	"C-suite" language
People	Roles and Responsibilities	Functionally defined	Multiple competencies
	Leadership	Command and control	Empowering and enabling
	Knowledge of the Business	Functional knowledge	Broad business understanding

Source: Booz Allen Hamilton

The Organizational Aspects of Convergence

There are a number of ways to address the organizational aspects of security convergence. They are:

- Combine both traditional and information security functions under one leader—Using this approach, convergence is assigned as a direct responsibility to one person, typically a security specialist from either discipline.
- Maintain both security functions as separate lines of responsibility and have them report to a common executive manager—Using this approach, the two security groups remain independent with separate budgets, etc., but they report to someone who is tasked with combining input from each separate security discipline and bringing the security message to executive management. The emphasis is on converged reporting rather than on converged operations.
- Keep functions separate yet facilitate knowledge enablement and information sharing by bringing the issues of security to an enterprise risk council—Using this approach, the risk council, with the participation of security executives, establishes responsibility for security decisions among the users of security services.

This publication examines the convergence and integration of security functions under the responsibility of a risk council as an effective approach to ERM.

2. The Role of ERM in the Convergence of Security Functions

The Definition of ERM

Ask a group of business leaders to define "enterprise risk management," and chances are each will offer a different definition and an opinion on who is involved. The most common features of the definitions that have been developed present ERM as being a coordinated process to manage the upside and downside of risk with the purpose of increasing value. Regulatory bodies and groups involved in ERM have added other features to the definition promoting the concept that ERM is a rigorous, continuous and proactive process that must be centrally implemented. With the developing importance of regulations on a global basis, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) has presented the definition that has been widely referenced and accepted.

> *Enterprise Risk Management is a process affected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity. It provides a framework to manage risk according to the organization's appetite and offers reasonable assurance regarding the achievement of its objectives.*[2]

Since risk management is so fundamental to management, most, if not all, organizations and their management would assert that they are already managing risk on an enterprisewide basis. The problem is that for many, their efforts are not coordinated or integrated across all risk areas. The true value of ERM lies in the benefits produced by a common, unifying framework for the many policies, processes, practices and organizational groups involved in risk measurement and risk management. It is this framework that structures the cross-functional collaboration that potentially results in improved agility and resilience, greater cohesion in the approach to risk management and, ultimately, in greater stakeholder value.

The Evolution of the Current Focus on Enterprise Risk

Managing risk has always been a fact of life for institutions, particularly financial institutions that profit by intentionally exposing their capital to credit and market risk. But what is it about the current landscape that is prompting more and more organizations to take a closer look at risk from an enterprisewide point of view? The answer lies in regulation, complexity, connectedness and market forces.

---

[2] Committee of Sponsoring Organizations of the Treadway Commission, *Enterprise Risk Management–Integrated Framework: Executive Summary*, 2004

Regulation

While there has always been regulation, the last decade could be characterized as the "era of regulation." The US Securities and Exchange Commission (SEC), Public Company Accounting Oversight Board (PCAOB) and New York Stock Exchange (NYSE) all require or encourage risk management-related activities. A renewed focus on the US Foreign Corrupt Practices Act of 1977 has further heightened awareness. The US Sarbanes-Oxley Act, introduced in 2002, has been called the single most important piece of legislation affecting corporate governance, financial disclosure and the practice of public accounting since the US securities laws of the early 1930s. Among other things, it imposes additional duties on corporate boards for the integrity of a company's financial controls.

In the financial services industry, the Basel II Capital Adequacy framework requires a more sophisticated approach to measuring credit and operational risk, and to determining the appropriate level of capital that banks need to hold against those risks. Complying with Basel II has required banks to find new ways of capturing more information about the risks assumed in their full range of exposure to market events and in their operations. As regulation becomes increasingly sophisticated, so too must the level of understanding and related responses from management and the board.

Complexity

There are numerous complexities to the contemporary global organization, some of which are relatively new to the business landscape. These include third parties, business partners, offshoring, outsourcing, and global operations across multiple regions, time zones, and growing regulatory requirements. The complexity of business models and relationships is driving the need for a more holistic approach to risk management.

Connectedness

It is becoming increasingly evident that business processes, risk and control across an organization are interrelated. The silo approach has proved inadequate since it leaves too many gaps and provides no credible means of understanding or being able to evaluate an organization's overall risk position. Some proponents of ERM have referred to it simply as common sense. In other words, when the organization begins to share risk and control knowledge systematically across its functions and departments, only then can the interconnectedness or correlations among risks be identified and managed. This is the essence of ERM.

Market Forces

Various forces have converged to push risk management into the consciousness of management and boards. The multimillion-dollar judgments in the Enron and WorldCom shareholder suits forced board members to draw upon personal assets to settle. As a result, there has been a

In the 21st century, with threats becoming more intelligent and more sophisticated, any program that looks at just one aspect of security is destined to result in a loss of value. Convergence is logical but we're not there yet. Convergence will depend upon the top-down perspective. The value of convergence has to be articulated in business language in C-suite level conversation. The C-suite will need to understand the financial impact of risk on earnings, share price and the like. And that will take the appropriate knowledge, skills and tools on the part of those who understand security and have the ability to understand the business impact as well.

Bill Boni, CISM
CISO, Motorola

scramble for education and understanding on the part of directors, doubtless hoping to avoid the necessity of digging into their own pockets. At the same time, stories of exorbitant severance amounts to executives who essentially failed in their duty to increase shareholder value have been splashed across newspapers and TV screens.

The Need for a Broader View

It is no longer meaningful to address risk in silos. All of the factors discussed previously have converged to demand a more holistic, enterprisewide view of risk. From an organizational standpoint, convergence of security functions may well be the most effective way to understand security risk.

Understandably, there is also a movement toward the convergence of security-related activities that has arisen in response to the increasing complexity and cross-disciplinary nature of today's challenges.

The convergence of traditional and information security is seen by some as an imperative. However, Deloitte's 2006 Global Security Survey found that the trend toward convergence "is still in its infancy, with many unresolved questions around the issue of successful organizational transformation." The survey found that 24 percent of respondents had experienced some form of convergence within their organizations and another 7 percent intend to deal with the issue within the next 24 months.

The need for a more encompassing enterprise view of risk calls for the participation of diverse functions, including human resources, traditional security, business continuity and information security. To capture the full benefit of convergence, there is a need to prepare security professionals for new roles, heightened responsibilities and an expanded mastery of complex business risk management.

The mission of enterprise security is to protect the assets of the enterprise in all of its forms (reputation, people, monetary, data, facilities). Security has a role to play in supporting growth by improving risk management related to growth activities such as entry into new markets, establishment of new alliances and the adoption of new business models.

The convergence of security functions would connect people, data and diverse systems. Convergence, by itself, is necessary but insufficient since it may merely mean that information is exchanged while decision making remains autonomous. The other necessary ingredient is integration in the form of improved intelligence sharing and

collaborative decision making. ERM has the potential to enhance and accelerate this integration. [3]

The Level of ERM Adoption

The realization that an ERM framework is becoming a necessity is illustrated in the AESRM survey by the fact that 35 percent of executives said that their company has a fully operational ERM program. One-third of the respondents said that their ERM program is in development, and 9 percent said that they are considering one. Roughly one-quarter of executives said their company either has not considered an ERM program or had decided not to implement one.

> *While 68 percent of respondents indicated that they have a fully operational ERM program or one under development, there was little consensus as to the objectives or goals of such a program and, consequently, what should be included as part of an ERM program.*

Among companies that have an ERM program, 52 percent said it has been in place for at least two years, while the remainder said that their program has been in place for a shorter span of time. More than two-thirds (69 percent) of executives at companies with an ERM program reported that there are five or fewer full-time-equivalent (FTE) staff members dedicated to the effort. Twenty-one percent of companies have between five and 25 FTEs in this area. In a few cases, the number of FTEs exceeds 25.

Executives reported a range of specific ERM implementation efforts. Between one-third and one-half of the executives said their organizations has implemented, or is in the early stages of rolling out, specific ERM efforts (see **figure 2**). These efforts include conducting formal enterprisewide risk assessments on a periodic basis (58 percent), aggregating risks at the corporate level (56 percent), developing enterprisewide risk policies and procedures (54 percent), and developing an enterprise risk dashboard/reporting process (51 percent).

While most executives whose organizations have not yet initiated an ERM program said that plans are under consideration or even in design, two areas are not being considered. Twenty-eight of the survey respondents said their organizations have no plans to establish a risk committee to oversee the management of all key risks. Twenty-eight percent claimed their organization has no plans to implement risk management and compliance knowledge sharing programs.

---

[3] Convergence may also address the coming together of protection technologies. The integration of physical devices and related security implications is discussed in the AESRM report, *Convergent Security Risks in Physical Security Systems and IT Infrastructures*, which can be obtained from the AESRM web site at *www.aesrm.org*.

Figure 2—Specific ERM Initiatives

Percent of respondents saying their company had either initiated or was in early stages of initiating action

Conduct formal corporatewide risk assessment on a periodic basis.	58%
Aggregate risks at the corporate level.	56%
Develop corporatewide risk policies and procedures.	54%
Develop an enterprise risk dashboard/reporting process.	51%
Establish a risk committee for all key risks.	49%
Develop and quantify risk appetite levels at corporate and business unit levels.	46%
Set corporate and business unit risk limits consistent with risk appetite levels for all major risks.	45%
Integrate risk management into other corporate practices.	37%
Develop knowledge sharing programs on risk management and compliance.	35%

The Scope of ERM Programs

Due possibly to the comprehensive nature of ERM, executives reported that their companies have adopted a range of definitions for the scope of their programs. For example, 55 percent of the executives indicated that their organization's ERM objective is to integrate risk management-related processes and practices across all risk types, 39 percent have a goal of integrating risk management across business lines, and 6 percent cited a desire to integrate risk management across geographic regions.

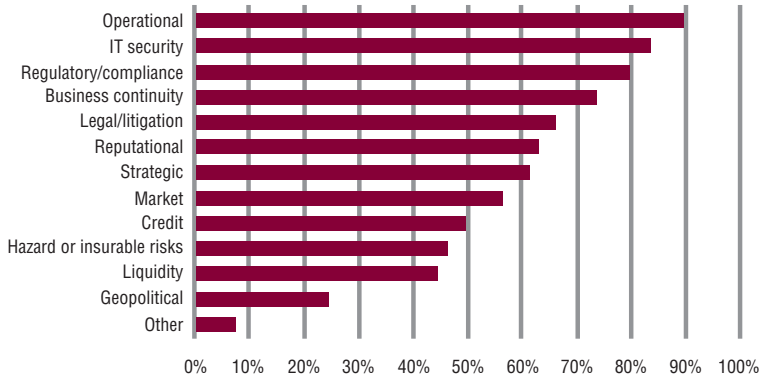
The types of risks included in the ERM program varied as well. In fact, only four types of risks were included by at least two-thirds of the executives. These are operational (90 percent), IT security (83 percent), regulatory/compliance (80 percent) and business continuity (73 percent) (see **figure 3**).

Most executives reported that their companies do not use a fully explicit risk assessment process. For example, only 33 percent said their company defines the kinds of risk it is willing to tolerate, while 52 percent said the kinds of risks it is willing to tolerate are partially defined. Furthermore, for those defined or partially defined risks, only 21 percent said their organization has defined its risk tolerance and 48 percent said risk tolerance has been only partially defined.

In addition, relatively few executives reported that their company has robust processes in place for monitoring and responding to risks. As an example:

- Just 19 percent of executives said their company has a robust process in place for identifying when risk tolerance approaches or exceeds defined limits, and 42 percent said this is partially the case.

Figure 3—Risks Included in an ERM Program



Results may not total 100 percent as respondents were allowed to select more than one answer.

- Thirty-three percent of executives said their organization has a robust process in place for correcting or escalating risks when they exceed defined limits, with 35 percent saying this is partially the case.
- Ninety-three percent of executives reported that their organization conducts annual training on risk management techniques. This training is provided only for specialists who perform specific risk management functions.

Security as a Component of ERM

ERM is primarily a top-down process that looks across the entire enterprise and improves its preparedness to identify and respond to risks that can either positively or negatively affect the organization. Success increasingly demands a holistic approach to risk management across the enterprise, and a means to coordinate risk identification, assessment and response. The process requires tools to better share relevant information on a timely basis with those who need to know, so they can do their jobs more effectively and efficiently. ERM can help address these challenges by providing risk intelligence for decision makers.

Risk intelligence relates to the capabilities for gathering, understanding, monitoring, reporting and responding to risks that may impact performance. For security risk, intelligence capabilities can be measured along the dimensions of governance, development and deployment of harmonized risk and compliance processes, risk identification, risk assessment, risk response, monitoring and escalation, control assurance and testing, risk intelligence performance and training, and sustainable and continuous process improvement.

For effective risk management, it is necessary to:
- Adopt a common operational framework
- Reduce autonomy while retaining authority
- Collaborate on all forms of enterprise security risks
- Provide better risk information for decision making
- Go beyond data sharing to collaborative planning and decision making

ERM is typically the approach an organization uses to harmonize, synchronize and rationalize its governance, risk and compliance activities. The current state of an organization's information security risk management convergence is typically a revealing snapshot of the state of its enterprise risk activities.

Based on anecdotal evidence, organizations often try to meet external requirements without enterprise prioritization or without considering how security risks correlate with other enterprise risks and their potential impacts. Funding for new initiatives continues to be more of a withdrawal from existing discretionary budgets than a strategic investment aligned with organizational goals and commitments. Most organizations continue to collect enterprise and security risk data many times (often from the same lines of business), assess and test many times, and transfer the results into reports to regulators and other interested parties. This practice continues to confuse lines of business, given their direct responsibility for value creation and value protection for the enterprise, and, more specifically, for security risk. This fragmented approach to managing governance, risk and compliance functions serves only to add to the ineffective and inefficient management of risk.

ERM seeks to rationalize and standardize practices for addressing all categories of risk, including security risk. This holistic approach is mirrored and supported by a broadening definition of security and the relevance of security to all parts of the extended enterprise.

As illustrated in **figure 4**, executives view security as encompassing a wide range of assets to be protected and capabilities to be enabled.

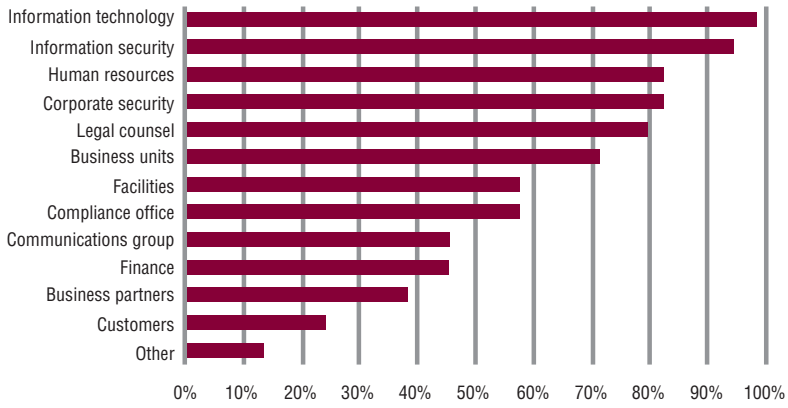
Figure 5 shows that executives see a utility value to security: it protects assets but is not directly involved in protecting customers or business partners, nor is it an influential part of decision making or used as a means to improve efficiency. In other words, security is seen as a tactical function that is not required or beneficial for higher-level business processes or decision making.

The threats that organizations are confronting, which are discussed in detail in the following section of the report, and enhanced regulatory oversight, as exemplified by Basel II, challenge the old way of thinking—one that works against security from being included in ERM.

Figure 4—How Executives and CEOs Define Security

Results may not total 100 percent as respondents were allowed to select more than one answer.

Figure 5—Areas or Functions That Participate in Security



Results may not total 100 percent as respondents were allowed to select more than one answer.

Adding to the complexity, more and more business partners are being asked to provide evidence of security contingencies and business continuity plans in their chain of business relationships. As seen in **figure 7**, disaster recovery/business continuity appears at the top of the list of operational initiatives for security. Furthermore, business continuity consistently figures prominently in response to other survey questions regarding initiatives included in integration and ERM programs.

The growing threat is coming from all sectors. It's coming from the common hacker who used to be fairly unsophisticated...all the way up to terrorists. The threat is growing to all of our networks just because of the growing capabilities of those who would wish us ill.

Paul de la Garza, Staff Writer
"War on Terrorism Turns to Information Network"
St. Petersburg Times, *January 2005*

3. The Way It Is

The Nature of Threats

Security incidents involving enterprise security are becoming more frequent and more sophisticated. Eighty percent of all major value losses are the result of the interaction of multiple risks, a factor that points to the need for understanding and managing the interrelationships among various risks.[4]

Organizations are experiencing a wide variety of threats, both internal and external. They include:
- Malicious attacks
- Employee misconduct
- Identity theft and account fraud
- Insider fraud
- Natural disasters
- Industrial espionage
- Physical/cyberterrorism
- Viruses/worms
- Geopolitical/nationalization of assets/repatriation of cash
- Intellectual property theft
- Brand attacks
- Supply chain disruption

While this list is not exhaustive, the scope demonstrates that threats come from many sources and involve different organizational resources and expertise to understand the nature of the threat and the protective measures that are required. The media is filled with stories that support the magnitude and impact of these risks. Breaches are pervasive, know no organizational boundaries, and happen at any time, usually with little or no warning.

In an attempt to keep pace with threats, more than 30 US states have passed laws requiring notice of security breaches. Several states now give consumers the right to enact "a security freeze"—the ability to stop any action related to credit, goods and services in new accounts that they believe might be false. But as fast as measures such as this are implemented, criminals who are becoming technologically sophisticated respond by launching new exploits that can keep security and business managers in an almost constant reactive posture.

[4] Deloitte Research, *Disarming the Value Killers*, 2005

Figure 6 illustrates the widespread impact of various security breaches, including one that has been referred to by the media as "the largest ever" to date. These breaches had a negative impact on virtually all functions and assets across the organization including brand/reputation/public relations, intellectual property, litigation supply chain, customer relations, finance and human resources, and often require a coordinated response by traditional and information security practitioners.

Figure 6—Security Breaches and the Scope of Their Impact Across Functions/Assets

Breach	Impact
A laptop containing the names and Social Security numbers of 29 million veterans disappears.	The breach of policy (an analyst removing his laptop from the work premises to take it home) will cost taxpayers at least US $100 million to notify affected veterans and provide them with credit-checking services.
Information is stolen from almost 48 million credit and debit cards during a computer breach at a well-known discount retailer.	Groups representing 300 banks file a class action law suit over the breach that involves personal data from millions of customers. At the time the lawsuit is filed, charges are still being made to the stolen credit card numbers. The breach is called "the largest ever" by the news media. The banks are seeking millions of US dollars in damages.
A computer tape with data from more than 200,000 customers is discovered missing at a third-party vendor's facilities.	Ironically, the data missing from a technology organization are not encrypted. While this causes immediate security issues, it also causes public relations issues with existing customers questioning the competence of the organization.
Hackers place malicious code at a credit card payment processor, which subsequently steals personal and payment data from the servers. Disclosure of the event forces the card payment processor to admit to holding certain card data in violation of the peripheral component interconnect (PCI) standard. Visa and American Express, whose transactions accounted for more than 80 percent of the payment processor's business, terminate their relationships.	The credit card payment processor files for Chapter 11 bankruptcy protection three months after the incident.
The private information of two million customers is stolen and used by malicious persons.	The company keeps the incident quiet for months before it gets out, resulting in general uproar from the public.
A human resources analyst's computer containing Social Security numbers and other private information belonging to 2,000 employees is stolen.	The company is forced to give affected employees a one-year subscription to a credit report service, allowing them to monitor their accounts for suspicious activity.

Figure 6 shows the functions/assets most impacted by the particular breach. In actuality, just about every breach, to varying degrees, has the following impacts:

- Customer attrition/decline in market share
- Brand/reputation damage
- Legal costs
- Regulatory costs
- Audit costs
- Lost productivity
- A detrimental effect on employee pride and morale, which affects retention and the ability to attract talent
- Financial cost (industry rule of thumb: loss of US $100 per stolen customer identity)

The Current Focus of Security Initiatives

When executives participating in the AESRM study were asked to name their company's top security initiatives for 2007, their responses were more focused on organizational and operational initiatives than on combating threat-based issues.

Asked to name the top five security initiatives they planned to focus on in 2007, the **operational** issue mentioned most often was disaster recovery/business continuity (66 percent). The **organizational** issue mentioned most often was security regulatory compliance, cited by 56 percent of the participants. (See **figures 7** and **8**.)

Figure 7—Operational Initiatives for 2007

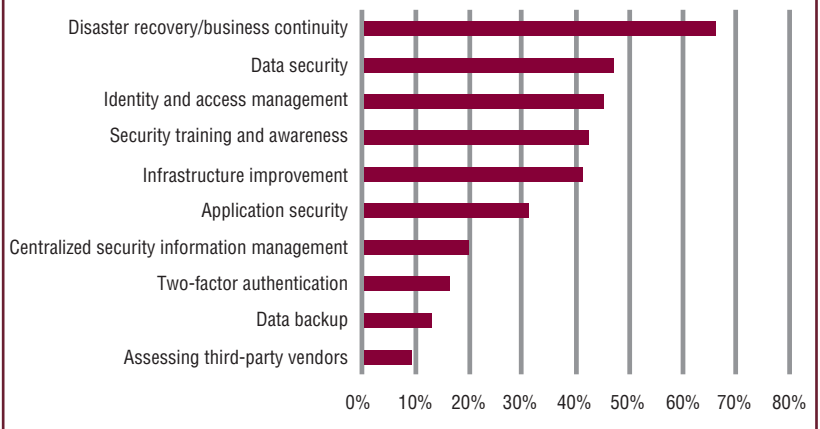
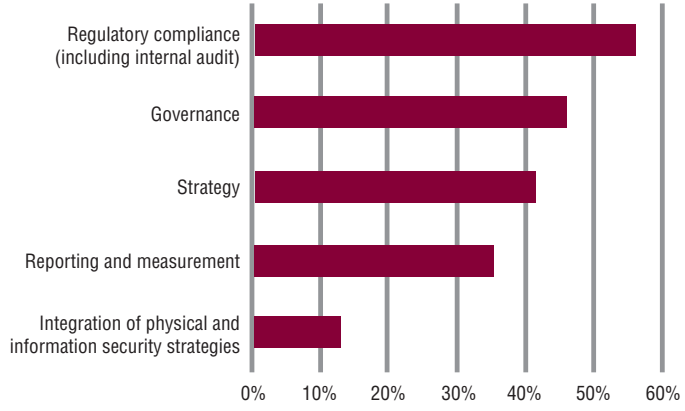
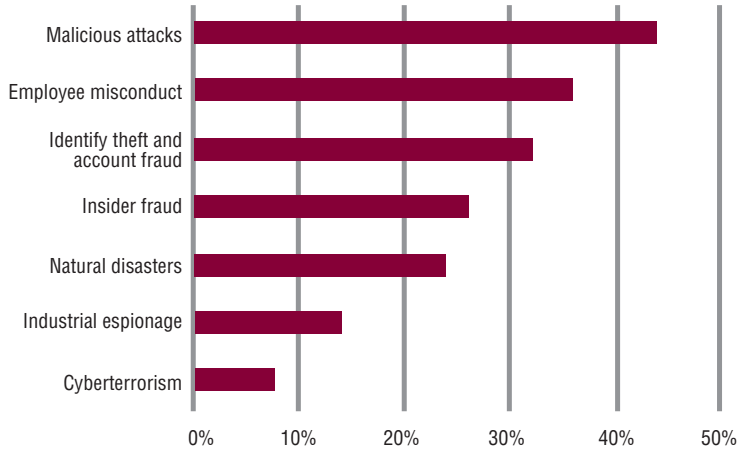


Figure 8—Organizational Initiatives for 2007



Although threat-based initiatives were not among the leading initiatives, they were mentioned by at least one-third of the executives (see **figure 9**).

Figure 9—Threat-based Initiatives for 2007



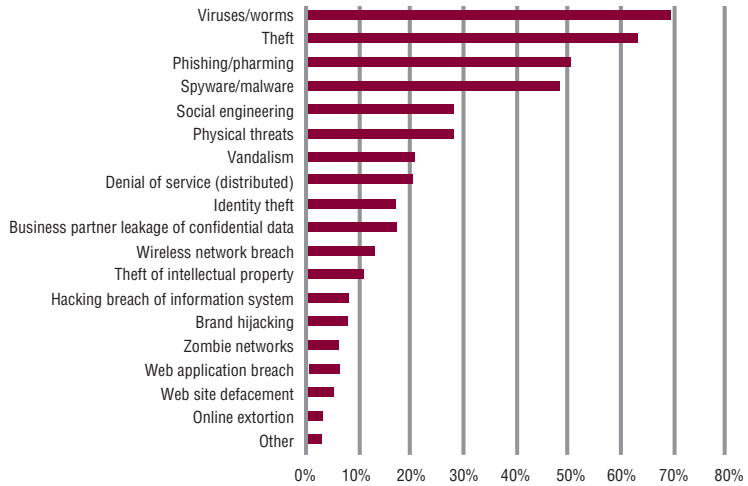
External and Internal Security Incidents

External Incidents

External incidents can be attributed to a compromise of physical security as well as a breach of information security. Respondents reported a wide variety of external attacks in the past 12 months.

The external attacks experienced most often were viruses/worm outbreaks (69 percent), theft (63 percent), phishing/pharming (50 percent), and spyware/malware outbreaks (48 percent) (see **figure 10**).

Figure 10—External Attacks Over the Last 12 Months



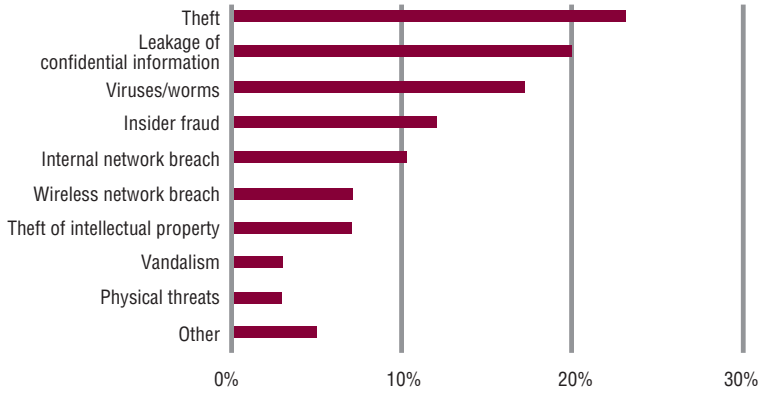
Results may not total 100 percent as respondents were allowed to select more than one answer.

Internal Incidents

Internal attacks were less reported in the AESRM study. They, too, often involve physical and data security issues and frequently require a coordinated response. Survey respondents indicated that their organizations have experienced internal attacks attributed to theft (23 percent), leakage of confidential data (20 percent), and viruses/worms (17 percent) (see **figure 11**).

Despite the wide variety of attacks on these organizations, efforts to combat them have met with some success, with damage kept to a minimum in terms of costs.

Figure 11—Internal Attacks Over the Last 12 Months



Results may not total 100 percent as respondents were allowed to select more than one answer.

However, it is clear that the future will bring an unprecedented range of new and evolving security challenges. The luxury of dealing with small, contained risks is a relic of a prior era. In the past, organizations could count on clearly delineated perimeters around physical and logical assets. Unfortunately, these defined boundaries no longer exist. Incidents can be motivated by politics or executed by organized crime rings operating on an international scale. In fact, the international nature of these crime rings is deliberate and calculated because it is much more difficult to investigate and prosecute "long distance" across jurisdictions with differing laws and justice systems.

As a result, management must now contend with risks that are often international in scope and cross multiple areas of security—factors that can quickly impact the shareholder value of any organization.

In response to the growth of threats and opportunities, it is necessary for an increasing number of practitioners representing different specialist disciplines within security to operate in a more coordinated manner. These practitioners may have already been involved in enterprise security, but their special knowledge and perspective have not been shared. Information security and corporate security, although working on similar issues, may rarely, if ever, meet to talk about what they are doing. This is clearly counterproductive, given that they provide similar services to the organization. For example, traditional security organizations often undertake corporate investigations but may not involve information security when computers or networks are involved. Information security, when investigating an incident, may not work with the traditional security personnel even though security personnel, in all likelihood, have valuable expertise in interviewing and the rules of evidence. The entire organization depends on human resources to perform proper

background investigations of new employees and to respond to employees who breach corporate policy. Background investigations and information concerning policy violations may not be shared with personnel in either the traditional or information security organizations.

As discussed previously, each party has an important role to play and each has deep, specialized experience, representing areas such as:
- Security governance
- Risk management
- Security principles and practices
- Physical security
- Information security
- Emergency practices and crisis management
- Investigations and computer forensics
- Intrusion and monitoring systems
- Personnel protection
- Legal issues
- Regulatory compliance

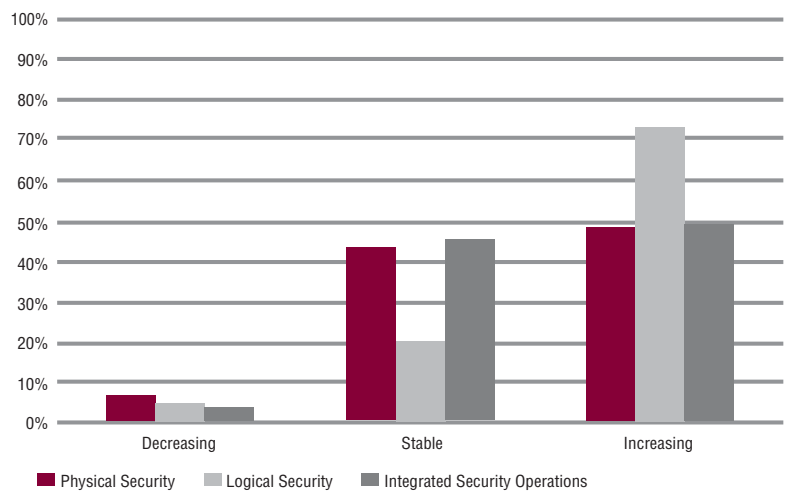
While these areas may have enterprise security as a common objective, they also have differing lexicons, focal points and approaches. It is these differences that create the potential for security gaps and redundancies that result in both vulnerabilities and higher costs. In addition, information flows are typically within the traditional silo structure, preventing a full understanding of risk interdependencies and compromising opportunities to contribute to effective solutions.

Against a backdrop of traditional structures and ingrained attitudes, two key questions arise:
- Can these differences in approach be reconciled to the benefit of the enterprise?
- Can cross-functional collaboration be improved to increase enterprise resilience to attacks and the agility to support growth in new markets?

4. The Value Proposition

Security budgets are increasing, as reported in the AESRM study, whether or not they are targeted to specific areas or to integration (see **figure 12**). However, key questions remain: do these expenditures bring increased value to the enterprise, do they contribute to the bottom line, and do they make the enterprise more responsive or competitive?

Figure 12—Budget Trends



When considering the wide scope of security impact, both across the enterprise and externally, it is easy to envision how improvements in security management could add significant value. This truth is evident not only for core business operations, but also in support functions.

For example, a recent study[5] focusing on business value resulting from supply chain security documents the following improvements:

- 38 percent reduction in theft/loss/pilferage
- 37 percent reduction in tampering
- 14 percent reduction in excess inventory
- 12 percent increase in reported on-time delivery
- 50 percent increase in access to supply chain data
- 30 percent increase in timeliness of shipping information
- 43 percent increase in automated handling of goods
- 30 percent reduction in process deviations
- 49 percent reduction in cargo delays
- 48 percent reduction in cargo inspections/examinations

[5] Deloitte Research, *Disarming the Value Killers*, 2005

There is a symbiotic relationship between physical data and logical data, but convergence of the two will not happen naturally. There are too many years of ingrained practices unique to each area. Sometimes you have to take a direct approach by assembling the right group of people and telling them what you want them to do and how you want them to do it.

David Morrow, CISM
Chief Security and Privacy Officer
EDS

- 29 percent reduction in transit time
- 28 percent reduction in delivery time window
- Close to 30 percent reduction in problem identification time, response time to problems and problem resolution time
- 26 percent reduction in customer attrition
- 20 percent increase in number of new customers

Clearly, improving security should not be perceived as an added expense, but rather a necessary one. Security pays dividends in many ways across the whole enterprise. A study by Deloitte[6] strongly supports this assertion. It found that corporate investments in secure commerce can go hand-in-hand with real, measurable business benefits. Specifically, the study expands upon the following areas:

- Cost reduction
- Enhanced revenues
- Better risk management
- Brand protection
- Market share preservation

Cost Reduction

Security investments can be used to drive more efficiency into the supply chain, and thereby lower costs and raise productivity. For example, one major public-private supply chain initiative, a cost saving of between US $378 and US $462 per container per shipment was realized from employing a mix of IT tools to secure and streamline shipping.

Enhanced Revenues

In addition to providing important security benefits, enabling technologies such as radio frequency identification (RFID) system tags can enable more timely and efficient information flows, thereby helping companies increase revenues by slashing the amount of time their goods are not out on store shelves.

Better Risk Management

Proactive security policies can help firms become more resilient by better managing the risks of a physical or information security incident.

[6] Deloitte Research, *Prospering in the Secure Economy*, 2004

Brand Protection

Security investments, especially in the areas of incident prevention and crisis response, can help to preserve and protect a brand—the most valuable asset for most companies. In addition, traditional security is highly involved in brand protection related to counterfeit products and product tampering. Software companies also have investigators who are intimately involved in virus and other malware incidents that are also related to brand.

Market Share Preservation

With various government and industry initiatives inducing retailers and manufacturers to require a higher level of security assurance from their suppliers, verifiable security practices will become obligatory for competing in the secure global marketplace.

The AESRM study found that one of the challenges that must be mastered to achieve value is "integrating security strategy across the enterprise." Rather than approach security in an uncoordinated and functionalized fashion, businesses need a top-down approach coordinated by a senior executive to optimize the effectiveness and efficiency of the overall security system.

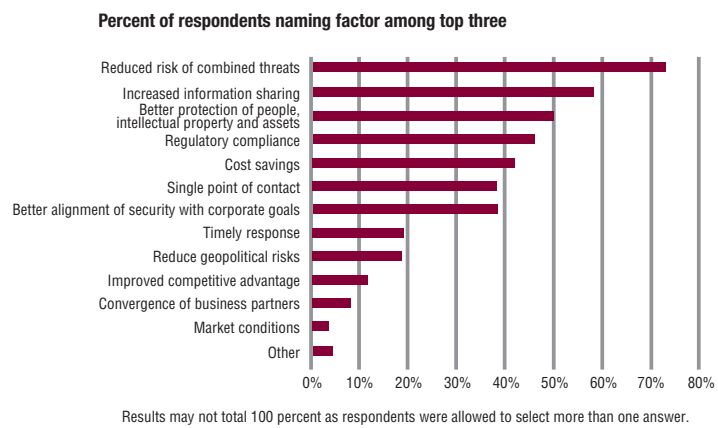
The integration of security management promises more than core benefits such as better protection of assets, reduced risk of combined threats, reduced costs and increased profitability. Ancillary value can be just as attractive, and these benefits include strengthened regulatory compliance, improved collaboration among business functions and improved information sharing.

When asked to identify the major drivers to their company's integration decision, respondents cited (**figure 13**):
- Reduced risk of combined information and physical security threats (73 percent)
- Increased information sharing (58 percent)
- Better protection of the organization's people, intellectual property and corporate assets (50 percent)

The responses also reflected a wide range of expected benefits beyond enhanced security (see **figure 14**).

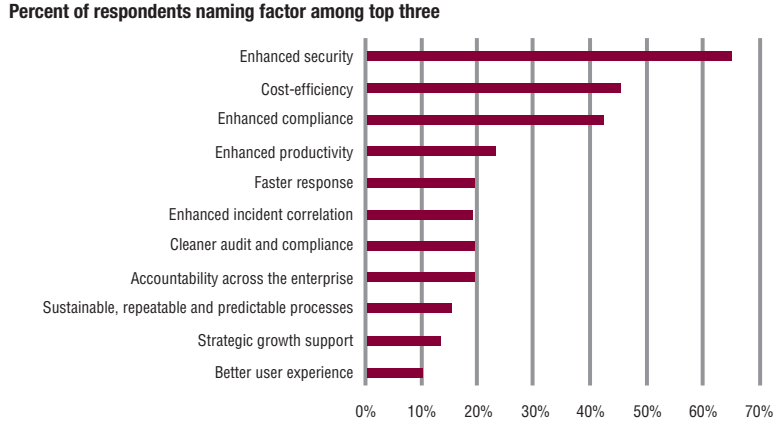
In light of these responses, it is apparent that security integration and ERM, when aligned, add value throughout the organization.

Figure 13—Most Important Drivers for Integration



Results may not total 100 percent as respondents were allowed to select more than one answer.

Figure 14—Most Important Value Propositions for Integration



Results may not total 100 percent as respondents were allowed to select more than one answer.

Although convergence is still in its early stages of adoption, those responding to the AESRM study indicated that tangible value has been derived from their convergence initiatives; however, thus far, security convergence has typically been driven by a single visionary executive. Indications are that the majority of organizations that converge do so for a common reason—to achieve value. Organizations have achieved value by creating efficiencies through their approach to managing risk, bringing cost reductions and time savings, and increasing operational effectiveness. Through this survey, respondents have indicated that cost and time

efficiencies were created by having faster and more effective incident response and increased productivity. The effectiveness of the convergence concept is created by introducing accountability throughout the organization and having sustainable, repeatable and predictable security processes across the enterprise.

Through the convergence of information and traditional security, organizations expect to achieve the overall benefit of enhanced security that can be translated into increased market opportunities, reduced risk and improvements in cost containment and time efficiencies. Yet, converting this proposition into a tangible reality poses significant challenges, as illustrated in the case studies in the last section of this report, And Now, the Reality: Case Studies from the Real World.

5. Convergence Models

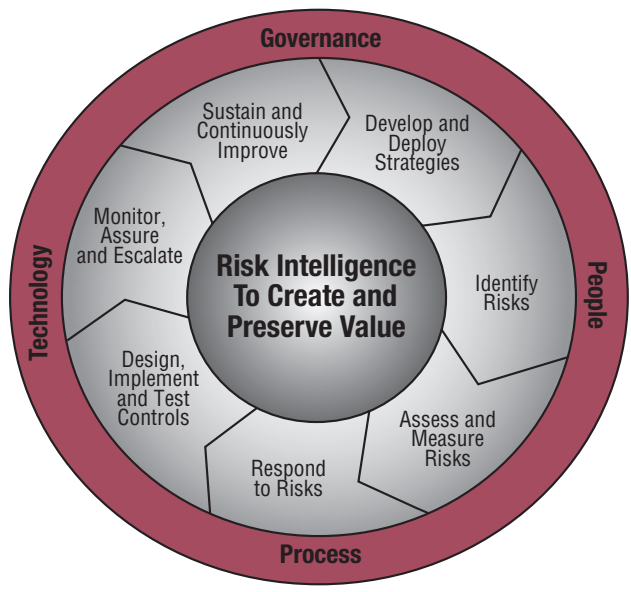
As demonstrated, it is logical to consider security convergence and integration in the wider context of ERM. Hence, convergence models presented here reflect a generalized risk intelligence ERM framework as developed by Deloitte to support organizations in their implementation efforts. The risk intelligence framework has been continuously refined based on experience from numerous client engagements. It forms the basis for understanding the components of ERM, how they interconnect, and how they can improve risk management efficiency and effectiveness.

A Framework for Risk Intelligence

At the core of the model (**figure 15**), risk intelligence is needed to create and preserve value. Risk intelligence means much more than simply the assembly and analysis of risk information, but rather the complete cycle of risk management from risk identification through deployment of strategies to address risks.

This cycle, depicted in the framework, contains the key components of a robust, enterprisewide approach. The approach, by design and necessity, incorporates the focused involvement of four pillars: people, process, technology and governance. Each of these must be organized and shaped with an enterprisewide perspective for optimal risk management performance and value.

Figure 15—The Risk Intelligence Framework



Among other things, governance defines how key decisions that affect the entire enterprise are made. This typically involves oversight of needed decisions and actions by governing bodies such as risk councils or a risk committee of the board, and supporting measures including policies, authorities, and charters. Governing bodies are responsible for determining the value-adding coordination that needs to take place between risk management silos, so that suboptimization is eliminated, if not reduced.

The areas governed are not limited to risk silos within the organization, but cover the enterprisewide scope of domains affecting all areas of the business and, therefore, all potential types of risk. These domains include enterprise strategies, the organizational segments of the enterprise, key processes that span organizational boundaries, systems that support all activity, and specific initiatives. Each of these areas is subject to unique risks, as are their interconnections, which tend to multiply the risks being faced and, thus, the need for sound governance overall. As the growth of various risks prompts increased convergence, it becomes increasingly necessary to manage this transition in a systematic manner.

Critical to this transition is the people factor. As owners and operators of functions with inherent risk, people need the right capabilities, competencies and credentials for risk management in this changing environment. Their roles and authorities must also be clearly defined and understood. Often, integration requires less autonomy within domains, as the need for collaboration across domains increases. For example, process design decisions should not be made in a vacuum with little regard for how other domains might be affected from a risk perspective. Similarly, systems technology decisions can impact how risks are managed and mitigated across many functions, and should be made in a well-coordinated fashion.

Within this governance, people, process and technology framework, risks are managed in an intelligent manner through a continuous cycle designed to create and preserve value. The starting point is, of course, that all risks are identified, including both rewarded and unrewarded risks. Rewarded risks are those for which the business exists—new markets, new products and services, new business models, and new alliances—those intended to increase growth and shareholder value. Unrewarded risks are those that pose only potential for loss and must be well managed to preserve value. These include the risks of security breaches, destruction or loss of assets, destruction of brand and reputation, as well as the risk of noncompliance with both internal and external regulatory and other binding requirements.

We are evolving from the Information Age to a new Age of Interdependence where information sharing and collaboration are required for making better decisions.

Lt. Gen. Harry D. Raduege, Jr.
Director of the Defense Information Systems Agency
Commander, Joint Task Force—Global Network Operations

The push toward convergence: certification and accreditation agreements
One example of innovative collaboration can be found in the United States in the joint initiatives of the National Director of National Intelligence (ONDI) and the Defense Department. They announced the agreement and implementation of seven areas of certification and accreditation for information technology. The seven areas include not only technical standards, but organizational, leadership, process, and operational initiatives to support convergence.

Jason Miller, "Agencies to Follow New IT Security Standards," Washington Technology

Once risks are thoughtfully identified, the next step in the risk intelligence cycle is risk assessment and measurement. Based on an understanding of the enterprise's exposure to risk, informed decisions about priorities and responses can be made. Response options include risk acceptance, mitigation or control, risk transfer, and risk avoidance. Criteria that support an integrated approach to managing all forms of risk should be established to guide the risk response decision process.

After risk response decisions are implemented, monitoring, testing and assurance mechanisms are critical to determining that the risk management strategies are operationalized effectively and sustained. These strategies include regular testing of mitigating controls, and monitoring, reporting, and escalation of risk incidents as appropriate. The assurance function is not limited to narrow risk areas but, more important, to assessing the ongoing performance of the entire risk intelligence framework from governance through the execution of required workflow activities of the people involved. Assurance reports can be used as a springboard for continuously improving risk management across the entire enterprise.

As risks are continuously identified and managed in this way, the risk portfolio serves as critical input to the development and deployment of new strategies. Informed decisions can be made as to where growth opportunities exist if certain risks are intelligently taken and managed, and where additional resources may need to be allocated to prevent or reduce the potential for unrewarded risk. Improved efficiency may be derived from the elimination of redundancy across risk and compliance functions. Coordinated risk responses are achieved, as opposed to *ad hoc* responses within functional silos. This framework provides the foundation for the development of a common lexicon for managing risk across the enterprise.

Consistency Among Information and Security Functions

There is little consistency in terms of the way in which organizations structure and staff their information and security functions. Of the participants in the AESRM study, only 41 percent of executives said their company has a single person who is responsible for overall security of the organization. Even more surprisingly, 31 percent of the executives said their organization does not have a chief information security officer (CISO), and 54 percent said there is no corporate security officer (CSO) or equivalent position.

Among companies that have an individual with overall responsibility for the integrated security function, there are a variety of different

executives playing this role, including the CISO (27 percent), CSO (27 percent) and chief risk officer (CRO) (12 percent). Thirty-four percent named other miscellaneous titles. Two-thirds of these executives said that the executive responsible for the integrated function reports to one of the company's C-suite executives, such as the chief executive officer (CEO), chief information officer (CIO) or chief operations officer (COO).

Convergence Models and the ERM Component

It is clear that ERM is beginning to be more widely adopted than convergence. It may well be that the concept of risk being assessed, aggregated and mitigated on an enterprisewide basis might have eventually come about on its own simply because of the logic of the underlying concept. But, clearly, the driver for ERM, to the level of importance that it has achieved to date, is a combination of factors including regulation of unprecedented importance and scope as well as complexity, connectedness and market forces.

There is no sign of things changing. Basel II, the most far-reaching regulation that the banking industry has experienced, and Solvency II, a similar operational risk management regulation for the insurance industry, are requirements within the 27 countries of the European Union and beyond. Complexity does not abate. Connectedness will become even more important, essentially mirroring the impact that globalization has brought. Market forces will continue to introduce ever more challenges. It is possible, then, that fullfledged convergence will not be a natural progression even though the underlying concept is logical. It is much more likely that security will be forced into some type of converged model by becoming a component of an overall ERM approach.

Risk Councils

Several ways that an organization can address convergence were identified in the introduction of this report, with risk councils being one of the most viable.

As organizations begin to implement ERM programs, key decision points related to regulatory and investor demands and possible risk events will determine the further evolution of the ERM program. These steps are frequently approved by risk councils or, where risk councils have not been formed, by relevant management councils. A risk council can be defined as a group of senior employees representing each of an organization's business units, internal audit, the "C-level" executive team, finance, legal and public relations, that is responsible for discussing risks, identifying potential exposures, and developing a program to control or mitigate significant risk from all sources.

Several key decisions are involved in implementing an ERM program:
- Confirming board and senior management active support and sponsorship
- Determining the right risk organization
- Developing and implementing a risk framework that aligns with business strategies and objectives
- Determining risk management and measurement goals and implementing "good practice" supporting processes and practices
- Determining the organization's risk-bearing capacity and setting risk appetite and limits

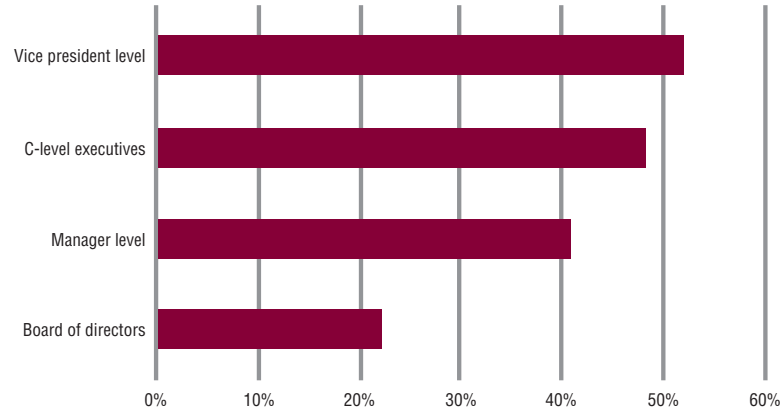
Risk councils often begin as "steering committees," evolving to more formal charters that aggregate existing risk specialist committees/councils. For example, the "hedging committee" combines with health and safety, environment management, and quality councils. Risk councils must have strategic senior management direction and support from the board of directors or other oversight body. In addition, they should align with the board's or other oversight body's risk competency. For example a general board committee assigns a specific risk area, such as executive compensation or security, to a specific board committee.

The AESRM survey addressed the governance structure companies use to address security management issues. Sixty-two percent of executives indicated that their organization has a risk council or equivalent, and 92 percent of those executives said they believe it has proven to be successful. Yet, only 32 percent of executives reported that their risk council has its own budget.

There was little consistency about who sits on the council, how regularly it meets and to whom it reports. (See **figures 16**, **17** and **18**.)
- Among companies that have a risk council, a majority of the respondents reported that no single title is held by the chair. The titles most frequently cited as the risk council chair are CRO (23 percent), chief financial officer (CFO) (15 percent), CEO (13 percent) and CISO (11 percent).
- Respondents were split on whether senior management and members of the board of directors participate in their risk council, or whether members are confined to less senior executives. Almost half of the executives (48 percent) said that there are C-level members on their risk council, while 52 percent said that it has participants at the level of vice president. In addition, roughly one-fifth (22 percent) of executives reported that their risk council also includes members of the board of directors.

The study also found that, for the most part, risk councils are perceived as successful.

Figure 16—Level of Participants on Risk Councils

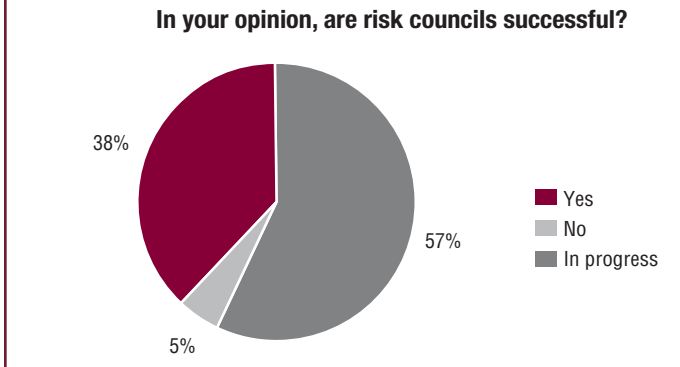


Results may not total 100 percent as respondents were allowed to select more than one answer.

Figure 17—Groups or Functions Participating in Risk Councils

Internal Audit	58%
Chief Financial Officer (CFO)	51%
Business Units	47%
Legal Counsel	38%
Chief Information Officer (CIO)	34%
Chief Risk Officer (CRO)	34%
Chief Information Security Officer (CISO)	32%
Chief Executive Officer (CEO)	30%
Chief Operations Officer (COO)	28%
Compliance Office	26%
Finance	26%
Human Resources	26%
General Counsel	23%
Corporate Security Officer (CSO)	21%
Chief Administration Officer (CAO)	15%
Board of Directors	13%
Information Security	13%
Information Technology	13%
Chief Techology Officer (CTO)	11%
Chief Privacy Officer (CPO)	6%
Corporate Security	4%
Facilities	4%
Information Technology Executive/Vice President	2%
Other	17%

Figure 18—The Perceived Success of Risk Councils



The reporting structure of the risk council members may also be integrated, with either dotted or solid line responsibilities, reporting to a common executive such as a CRO. Fundamentally, organizations must be motivated to collaborate for optimum effectiveness.

In addressing the need to manage enterprise risk, each organization needs to take an approach that best suits its unique culture and structure. This may involve using the concept of a risk council while, at the same time, creating a structure that is unique. For example, a major US financial services company addresses enterprise risk councils and the convergence of security functions as follows:

- "Stewardship" has evolved, in which heads of traditional security functions are designated as "risk stewards," along with leaders of other risk functions. For example, in the security arena, the enterprise has a physical security steward and an information protection steward.
- Risk stewards share accountability for "border risks" among risk functions. They must have agreement from the impacted risk stewards before any initiative is implemented affecting multiple risk functions.
- This has naturally led to the formation of a risk council comprised of risk stewards and chaired by a risk steward or, sometimes, by a leader from the ERM function, as the need arises to address major issues.
- One of the roles of the ERM function is a responsibility to support the risk stewards. This is accomplished by providing risk management and governance methodologies and tools, providing recommendations for infrastructure deployment to support risk management, evaluating issues, and escalating issues to the board as appropriate.

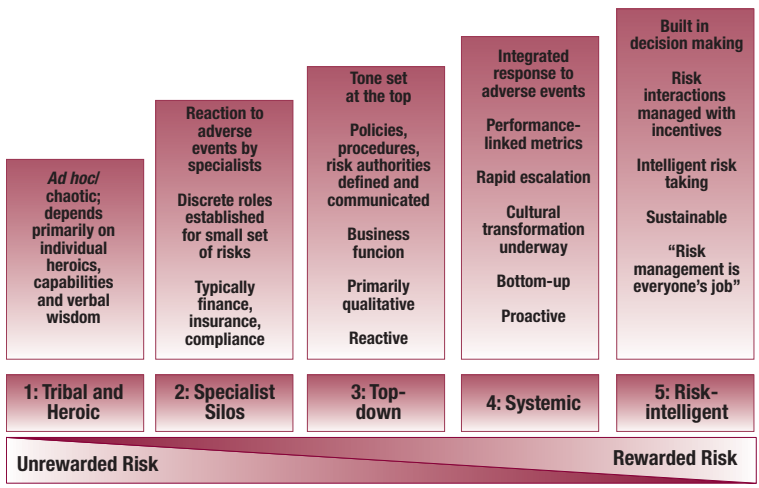
This example shows the diversity of approaches that can be taken. While the approaches implemented within organizations may differ, the benefits are obtained when a wider perspective of risk drives greater coordination and cooperation, and traditional silos of influence and authority are eliminated.

6. ERM and the Risk Intelligence Capability Maturity Model©

Achieving the optimal value from risk intelligence requires an understanding of, and sensitivity to, the cultural factors of the organization. As this study and others illustrate, organization culture consistently tops the list of barriers to ERM implementation. To address this central concern, Deloitte has combined key cultural factors with aspects of ERM deployment into a Risk Intelligence Capability Maturity Model©. This tool serves not only to assess and monitor an organization's cultural position regarding its capability to effectively implement ERM, but also serves as a vehicle for developing short- and long-term plans for risk intelligence deployment.

As depicted in **figure 19**, risk intelligence capability maturity is measured along five levels of maturity, in order of increasing risk intelligence. In today's business environment, many organizations find themselves at level 2, relying on specialist silos such as security, finance, insurance and compliance to manage risks on behalf of the enterprise. However, upon experiencing the drive toward convergence and integration, organizations react by moving into level 3, a top-down approach, which is driven by mandates, policies and the establishment of new risk authority functions from the top.

Figure 19—Risk Intelligence Capability Maturity Model®



Although level 3 is a logical and essential next step, the model depicts the ultimate risk-intelligent organization as one in which "risk management is everyone's job," not simply an additional task mandated by executive leadership. At this level, risk management is thoroughly integrated throughout its people, processes and technology, and its governance structure

utilizes and motivates the most appropriate and effective tools for management and monitoring of risks across the enterprise. This degree of risk management capability maturity enables the transition toward rewarding intelligent risk taking that, in turn, increases value for all stakeholders.

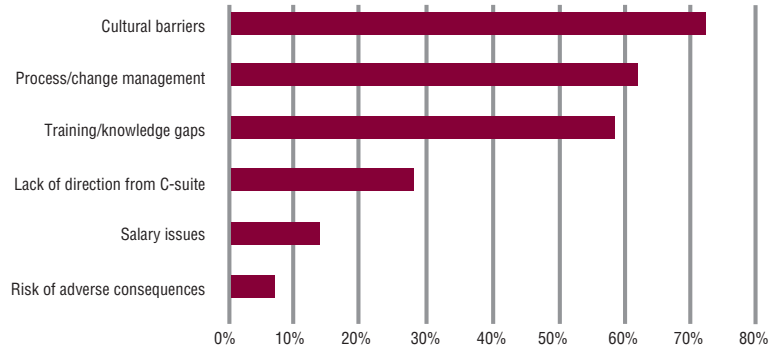
The Risk Intelligence Capability Maturity Model, while designed to help businesses manage the full spectrum of risks they face on a daily basis, is clearly in alignment with the operating culture obstacles faced by the convergence of security functions. It also portrays the desired paths that organizations must take to integrate security functions and incorporate them into a holistic risk management methodology.

Risk intelligence and capability maturity also enable organizations to address the information-sharing paradox faced by security professionals. A mature risk culture with a well-designed system for managing risk information is structured and rewarded for sharing appropriate information to support risk management goals.

7. Barriers and Success Factors

The AESRM study looked at obstacles to integration (see **figure 20**) and identified cultural barriers, process/change management and training/knowledge gaps as the top three obstacles to integration.

Figure 20—Obstacles to Integration



Results may not total 100 percent as respondents were allowed to select more than one answer.

Increased information sharing as a driver to integration also poses a barrier to integration since it represents a fundamental paradox in security management: information must be shared with insiders and simultaneously restricted to outsiders. Within the context of ERM, traditional outsiders may become associates in risk management and, as a result, become insiders. This paradox is not limited to information sharing since integration also calls for sharing of other resources such as people, technology and tools. Further barriers to effective integration are identified in **figure 21**.

Convergence Hurdles: Cultural Differences and Cross-training

With the implementation of any new business concept, organizations will inevitably encounter obstacles. The top two obstacles for people were identified in the AESRM survey as operating culture and training and knowledge gaps.

Information and traditional security personnel are accustomed to their unique "mind sets." In striving to achieve separate departmental goals, each function draws on the skills, expertise and tools it has traditionally used. Within independent silos, the goal may be similar but the solution will be unique and, in most cases, incomplete as threats increasingly cross departmental boundaries. The primary challenge for any organization contemplating convergence is to get separate security functions to work collaboratively.

Figure 21—Barriers to Effective Integration

	Barriers	Success Factors
Governance	• Lack of enterprisewide perspective and ownership • Functionally focused management	• Leadership with enterprisewide perspective and accountability • Management alignment for enterprisewide performance
People	• Operating culture barriers—organizational impediments and reluctance to share information across functional boundaries • Training and knowledge gaps • Lack of accreditation and certification	• Communication strategy and execution—common framework, terminology and incentives to break down organizational barriers and improve collaboration
Process	• Lack of end-to-end process ownership and measurement • Inconsistent subprocess objectives • Suboptimized process design • Unanticipated process requirements from external forces such as market pressures and regulatory requirements	• Clearly defined end-to-end process ownership and measurement • End-to-end process design and improvement • Agile and resilient processes
Technology	• Ever-changing technology • Incompatible systems • Inconsistent standards • Increasing sophistication and complexity • Lack of interoperability	• Robust framework that supports constant change and increasing complexity • Commonly agreed-upon standards • Enterprisewide systems design

Respondents to the AESRM survey revealed that "closing the knowledge gap" can best be accomplished through training. However, they are finding it difficult to transform highly focused specialists into broader-thinking generalists who take on a wider role with respect to security. Personnel in each function generally come from different professional and educational backgrounds. It is not clear if teaching IT skills to a physical security specialist with no IT background is easier than training an information security professional in physical security concepts and technologies.

Cultural Barriers

The majority of organizations deem operating culture barriers to be the main challenge in converging traditional and information security functions into one overall corporate security strategy. The functional staff within traditional and information security specialties are often protective of their current roles, responsibilities and intellectual property. Integration, some people fear, may mean the loss of jobs.

Organizations are also finding that traditional and information security staff may be hesitant to report to new management. Cultural barriers are major obstacles. Independent security functions can be reluctant to give up control when they believe they could lose budget, organizational influence and resources.

Within the various functions, personnel are measured and rewarded based on different parameters. If these functions converge, it could be difficult to work toward an overall corporate security strategy if the personnel involved are being measured and rewarded based on different parameters. Organizations could face difficulty in aligning their integrated security goals with corporate goals to accommodate the objectives outlined by the two different operating cultures.

Training and Knowledge Gaps

Another challenge that organizations might face when implementing an integrated security strategy is overcoming the training and knowledge gaps of traditional and information security staff. As part of convergence, personnel will be required to adopt different roles and responsibilities. Traditional and information security personnel often come from differing educational and professional backgrounds. Traditional security staff, who are primarily concerned with protecting an organization's tangible assets and people, often come from a background in law enforcement, the military or law. These people generally do not have deep experience in IT-related technical skills. Information security staff, who are typically more concerned with protecting an organization's information infrastructure, come to their positions with application development, systems and networking expertise. Although information security specialists have strong technical skills, they do not have experience in significant areas of protection such as surveillance, investigations, crisis management, personnel security and facilities protection. While the expertise of traditional and information security specialists differs, the unifying factors that drive both disciplines are the protection of the enterprise and the management of risk. Organizations may need to identify knowledge gaps and opportunities for cross-training. Training investments will help staff transition to new roles as an integrated function, while maintaining the balance between generalists and specialists.

Training does not necessarily apply only to the need to take on new roles. Training may also involve a redirection of experience that already exists. For example, security guards making their rounds in a building can be prepared to look for potential IT security problems such as passwords taped to walls or computers left on. Facilities people can be made aware that computers being discarded may still contain sensitive information, and the resulting action can be integrated into a standard based on an approved method of disposal or destruction.

With advances in physical security and the increasing dependence on digital systems, traditional security personnel need to be prepared to understand the risks involved with transitioning from a closed systems environment to an open networked and increasingly wireless environment. This may well be intimidating for some. New security systems increasingly require the acquisition of different strategies and techniques that have not been traditionally required for staff involved in physical security. The procurement, deployment and maintenance of the new digital controls require the specialist technical knowledge and skills of IT personnel. Similarly, there is frequently a physical security knowledge gap among IT personnel, suggesting that both information and physical security personnel should be trained to work cross-functionally.

External factors also present barriers while acting as drivers for remediation and successful integration. For example, new regulatory requirements triggered by breaches in security pose challenges to organizations. However, in the process, organizations discover that they are naturally gravitating toward a more integrated approach in order to adjust to the new demands.

The evolution to a more converged model of security requires effective change management. As reported in the AESRM study, companies use a variety of change management techniques when converging security functions (see **figure 22**). The initiatives used most often are leadership alignment (31 percent), communications strategy and execution (28 percent) and organizational design (26 percent).

Figure 22—Change Management Activities Required to Integrate

Results may not total 100 percent as respondents were allowed to select more than one answer.

Realistically, the barriers can be difficult to overcome, regardless of the change management approach and initiatives used. An integrated approach to security—and, to a greater extent, an enterprisewide approach to managing all risks—must overcome some cultural norms that may have been entrenched, in some cases, for decades. Personnel from certain functions may be reluctant to participate productively in working sessions with sister functions, largely because they have never done so before, do not speak the same technical language, have trouble understanding the other's perspective, and have little institutionalized motivation or self-interest to cooperate in such an initiative.

There is also a need for all persons to embrace a broader perspective. Facilitation, negotiation and leadership skills are needed, as well as the ability to understand and communicate the issues encountered by multiple risk areas. The organization's political environment can also play a major role since certain key leaders may view the integration initiative as a threat to their position within the organization. Human resources, information systems, policy, and governance tools and processes will likely have to be adjusted. Without a major motivator, some may find these obstacles insurmountable.

Elimination of Barriers Does Not Necessarily Equal Success

Success in convergence does not necessarily happen when all of the barriers are eliminated. Strong catalysts and enablers are needed to sustain the elimination of the barriers, which cannot happen without the commitment of resources. The catalyst can come from a strong, visionary executive in a key role, government scrutiny of operations, or a significant security lapse resulting in nearly catastrophic consequences. Once the catalyst triggers the drive for integration, an appropriate convergence model needs to take hold for prolonged and effective success.

8. And Now, the Reality: Case Studies From the Real World

These case studies from the real world are presented in an order that reflects a progression from the simplest converged function to a full-blown, ERM-integrated solution.

Case Study 1. Constellation Energy Group

Issue

As the oldest utility company in the United States, Constellation Energy Group (Constellation) owns and operates 37 fossil fuel power plants and three nuclear power plants, utilizing approximately 12,000 full-time employees and a few thousand contract employees. John Petruzzi, Director of Enterprise Security at Constellation, was hired to manage the operational risks of the organization in the aftermath of the Enron debacle and impending regulation. John had two goals:

- Deliver the posture of the organization to executive management whenever needed
- Show that his team was delivering true value

Solution

At Constellation, the overall enterprise security group falls into the larger ERM group, which has a direct reporting line into its CRO and senior vice president. Currently, there are four operational units or "buckets" that report directly to John: information risk, enterprise operation, access management and compliance management.

John focused on three factors that he said are the keys to the success of the program:

- **Communication**—People know what is happening and why at every stage.
- **Collaboration**—The appropriate people are on board early in the process, a strategic move usually referred to as "upper management buy-in," and an absolute necessity for any successful business initiative.
- **A dynamic team of security professionals**—People are aligned by business units that fit their qualifications. Then, contingent staff members, either process- or technology-specific, are used to assist them.

Results

Executives get a real-time view of the organization's risk, financially and operationally.

Case Study 2. SAP

Issue

SAP is the one of the world's largest business software companies, with more than 200 locations in more than 50 countries. Headquartered in Walldorf, Germany, SAP employs more than 38,000 people globally. SAP gives many of the responsibilities traditionally reserved for management to its employees, who have become effective and proactive at making important business decisions.

The problem was that there was no centralized security policy and no governing body providing rules and guidance to the nearly 100 employees for whom security was the main responsibility. As a result, there were various groups performing their own security activities—activities that may or may not have been aligned with corporate strategy.

Solution

Three years ago, SAP undertook a large integration project aimed at combining the existing information security and physical security teams into one global security organization. SAP also introduced a corporate security department that is primarily responsible for the strategic aspects of security. The virtual security team is made up of more than 80 security professionals (logical and physical) who have the role of security officer in addition to their business line responsibilities.

The security officers are governed by a corporate security group of 14 employees who provide guidance, awareness training, strategies, requirements and solutions as well as set the baselines for security in an effort to maintain consistency within SAP globally. Each of the security officers is responsible for all aspects of physical and information security within his/her respective function and is expected to comply with the guidelines set by the security steering committee, a committee that includes some board members and acts as the final "head" of security in the organization.

Results

While the global security organization is responsible for providing information regarding security risk, SAP has defined a separate global risk management group, which has about 80 full-time employees working only on risk management. Since security is not the only area of an organization that risk pertains to, businesses need to be constantly aware of all risks that face the organization—from operational risk, which includes a large aspect of information and physical security, to financial risk, which may include risks associated with foreign exchange rates or liquidity and cash flow.

Lessons Learned

As SAP has demonstrated, the convergence of physical and information security does not necessarily have to be a daunting task. Communication and culture played major roles in the integration of these two aspects of security. As with any major organizational change, understanding why people behave the way they do, why they may be opposed to change, and how to overcome their resistance to change, is of utmost importance.

Case Study 3. Diversified Manufacturer

Issue

The company examined its existing risk management practice to gauge how well its risk capability served the company's current business objectives. Results of an initial risk assessment revealed significant issues:

- Timely information on key enterprise risks was not available under its current system.
- Risk management was practiced disparately in business units.
- No standardized processing or reporting on risk existed.
- At the enterprise level, risk management was practiced informally.

Acting on the assessment, the company's leadership coalesced on a plan to realign its risk management practice with its business strategy. The company designated ERM as a business imperative, initiated a strategy to build its risk management capability, improved its state of risk management and learned how to increase its risk intelligence.

Solution

The company implemented an integrated and intelligent ERM framework designed to:

- Identify, assess, evaluate, report and manage various types of risks (such as financial, operational and strategic) across business units
- Use the existing enterprisewide Six Sigma management process to roll out integrated risk management practices
- Introduce risk assessment techniques to better calculate the impact of risks on enterprise value, in turn providing risk intelligence to inform decision making
- Develop organizational approaches (working with existing business groups and processes) to monitor and mitigate risk across industries and geographies
- Establish clear reporting channels to communicate risk so information on risk could travel to and from business units, senior management, the audit committee and the board of directors. In other words, risk intelligence could be delivered quickly and easily to all levels of the organization.

Results

With a comprehensive risk assessment and risk management training, key enterprise risks from business units could be identified and singled out. The company's management acquired the "big picture" on its risks so that resources could be appropriately allocated. The company's ERM practice could now produce ongoing benefits and advantages. Several stand out:

- Increased risk awareness among business units
- Improved risk management capabilities, increasing the overall risk intelligence of the organization
- Updated risk mitigation plans across the enterprise
- Integrated and organized regulatory and compliance programs to form one group; as a result, the group produces consistent and sound risk information, increasing management's awareness of critical risks
- Adopted processes to incorporate timely risk information into strategic planning
- 10K reports prepared efficiently and effectively
- Synchronized ERM priorities with internal audit planning and assessments

Lessons Learned

With firsthand experience—and success—in the implementation of its integrated ERM program, the company offers some insightful recommendations:

- Secure buy-in from management and key parties. Drive the ERM program from the top down—this includes the board of directors, the C-suite and senior managers.
- Delineate clear roles and responsibilities, e.g., assign executive risk owners and risk-intelligent process facilitators.
- Utilize an enterprisewide accepted practice or approach (such as Six Sigma) to embed risk intelligence practices into existing processes.
- Start small with a single business unit and roll it out gradually.
- Encourage cross-functional collaboration and teamwork across business units to overcome potential resistance in the organization.
- Promote and use standardized processes and tools to identify, collect and report risks.
- Articulate the benefits of an intelligent ERM program regularly.
- Obtain external help if internal resources are constrained. Engage advisors to introduce leading practices.
- Consider internal and external risks and link them to business strategy and performance management.
- Improve the ERM program continuously to achieve the benefits associated with sustainable and intelligent risk management, including improved strategic "reflexes" to respond to emerging risks and opportunities in the marketplace.

Case Study 4. Global Marketer, Producer and Distributor of Consumer Goods

Issues

The existing ERM program was described as the "road to nowhere." The organization needed an assessment of current ERM initiatives compared to leading practices to gain executive and operating unit buy-in. It realized the need for a comprehensive road map for ERM for deployment across the organization.

Solution

The enterprise's solution was to:

- Use recent thought leadership and experience in developing ERM services that are part of the executive management process
- Make extensive use of specific industry and cross-industry knowledge and experience to facilitate executive buy-in
- Demonstrate to executives the value added by risk assessment, response, monitoring and communications
- Develop and enhance a culture of communication and collaboration among business units relative to risk management
- Begin to develop and deploy tools to identify risk, assess risk management capability and link these to key value drivers

Results

As a result of the above activities, the company was able to:

- Identify a process or methodology that promotes action so that critical issues are raised quickly to senior management and the board of directors
- Offered recommendations to improve the effectiveness of the company's ERM initiative including organizational structure, leadership involvement and project management
- Develop a road map to successfully lead the company from its current state to the desired future state
- Embed the cycle of risk identification, assessment, response and monitoring in the organization's standard strategic planning and budgeting processes

Lessons Learned

The following items were identified as critical to the success of the project:

- Listening to the needs of executives and following up with them in a consistent, thoughtful manner
- Providing the best resources available and working with executive teams throughout the entire process, end to end
- Providing a well-thought-out road map that details the steps needed to implement a sustainable, ongoing ERM program

Case Study 5. City of Vancouver, BC, Canada

Issue

About three years ago, Dave Tyson, then head of information technology security for the City of Vancouver, was charged with the task of managing the physical security team in addition to his current responsibilities. Tyson did not feel as though he had the capacity to manage both the physical and information security aspects of the City of Vancouver in the siloed manner in which they were currently running. The groups had different reporting structures, different budgets and, most important, different expectations from upper management. These differences, combined with the number of task duplications that existed between the groups, led Tyson to one conclusion: converge the physical and information security functions into one enterprise security function.

Solution

Tyson proposed his convergence strategy to upper management using three benefits that he felt a converged function could deliver to the business:

1. **Cost reduction**—By combining the two functions, the organization could save money by reducing the number of duplicated tasks, effectively "killing two birds with one stone" by combining the risk assessments and audits that had previously been performed separately for physical and logical threats.
2. **Increased risk mitigation**—Tyson's strategy was based around the idea that the threats the organization faces on a day-to-day basis are already "converged." That is, it is extremely difficult to divide current threats into two distinct groups such as logical and physical. Rather, by combining the two security groups, Tyson argued that the organization would be in a much better position to identify the threats and mitigate the risks that "straddle" the two security functions.
3. **Organizational simplification and reduced duplication**—As the organization stood at that time, both the physical security manager and the IT security manager reported to the director of business support operations. By combining the two functions, it would be possible to cut reporting by nearly 50 percent and increase the value of the reporting by adding insight into further risk mitigation strategies as outlined in the second benefit point.

Results

The result of Tyson's proposal is the enterprise security team at the City of Vancouver. According to Tyson, the team plays more of a governance role than an operational role, by providing security policies and guidelines that are used by the operational teams (system administrators, firewall administrators, etc.) on a day-to-day basis.

Tyson has been able to demonstrate tangible value to the organization in a number of ways. In the first 90 days, IT security desktop policy violations were reduced by 54 percent, at no cost to the organization.

Convergence has also allowed the security function to save money that would have otherwise been spent needlessly. It has recently begun using its existing storage area network (SAN) architecture to store digital video feeds that monitor physical security. According to Tyson, SAN storage costs are one-third that of digital media storage costs. Tyson also recalls a recent situation in which the physical security team proposed installing new fiber optic lines that would be used to transmit a live feed from more than 700 video cameras around the city. The converged solution: use the already existent fiber-based local area network (LAN) with a technology known as virtual local area network (VLAN) to accomplish the same task with virtually no overhead costs.

Lessons Learned

Tyson identified the following as lessons learned from the project:

- Determine that there is an adequate execution of strategy across all levels of the enterprise. Either Tyson, or a member of his team, sits on the steering committee for all major IT projects that are proposed. From there, they can determine that the appropriate activities and controls are in place to obtain the required level of physical and information security. As part of this role, Tyson also helps define the project and drive the requirements for all deliverables. To determine that security practices have been followed accordingly, the team conducts security audits throughout the project as well as on the final deliverables.
- Determine that the team's skills and competencies remain current. Third-party relationships can bring value to an organization. It is important to maintain a strong relationship with a number of providers; they can provide resources that are up to date and deliver high-quality work in a timely fashion to meet security requirements.
- Recognize that the most critical success factor is an understanding of the different cultures that exist between the groups. During a consolidation effort, it is crucial to be cognizant that there are two groups of people who may or may not have an understanding of the other group's functions, goals or capabilities. It is critical to communicate to both groups and explain to each how the two groups fit together, their similarities and the benefits of consolidation. Ideally, the communication can be done in a language that is understood by both groups, thus easing the process of convergence significantly.
- Focus on small wins in the beginning. Attacking the low hanging fruit areas first makes it much easier to demonstrate value to management and further grow the initiative.

- Recognize that the battle is never completely over. Moving forward, Tyson is looking to better institutionalize convergence as well as formalize some outstanding documentation, including integrating the charters of physical and information security, and harmonizing the budget to one enterprise security budget rather than having separate physical and IT security budgets.
- Look for ways to improve the reporting abilities of the team. Consider an executive dashboard that will provide a high-level review of the current security status of the organization, but will also incorporate the ability for executives to drill down easily into details such as specific security breaches or incidents. Establishment of a risk council can further increase the value that a converged group can deliver to the organization.

9. Conclusion

The convergence of traditional and information security functions is a concept that, outside of a few visionary organizations, would have been unfathomable in the early 1990s. Today, even though the concept is still in its infancy from an implementation standpoint, the topic is written and talked about with increasing frequency and enthusiasm. It is evident, based on the research summarized in this report, that convergence will happen even though its time may not be the present. According to a "state of the CSO" survey conducted every spring by Deloitte, the overall trend toward consolidated departments has been upward for at least the last three years.

True convergence of traditional and information security involves disciplined cooperation between previously separate security functions. It means working together in a results-oriented effort to achieve the objectives of the organization. It is not simply merging the information security group and the corporate or physical security group on the organizational chart. In other words, true convergence is mainly about substance, not just about form.

There are a number of driving factors behind convergence, most of which require, to varying degrees, that the organization be able to understand, measure and mitigate its significant risk. These factors drive the need for a framework for ERM that will, in turn, help to drive convergence. Analysts predict that the convergence market will grow rapidly during the next five years as ERM points more organizations to greater security efficiencies and opportunities to strengthen effectiveness.

This report suggests that there are essentially three ways to structure convergence: combine both functions under one leader, maintain separate functions and have them report to a common manager, or keep the functions separate but bring the issues of security into an enterprise risk council. In this survey, 62 percent of executives indicated that their organization has a risk council or equivalent and 92 percent of executives said they believed it has proven to be successful. Despite budgetary issues and confusion as to who is part of the risk council, the risk council concept is clearly the place to begin the process of convergence.

Why have some organizations adopted the convergence approach already? Survey results show that convergence within an organization is often spurred by the vision of one person. These visionaries, aside from being executives, have a strong belief in the benefits of convergence, and have the personal commitment to see their idea to completion despite the uncharted territory in which they may find themselves.

There may well come a time when the convergence of security is commonplace and the employees of a future era cannot conceive of the two security functions ever having been managed in silos. It may well be, too, that the converged security model they use is one that has been originated by one of the visionaries of these case studies.

The Alliance for Enterprise
Security Risk Management℠

The Alliance for Enterprise Security Risk Management (AESRM) was formed in February 2005 to encourage board- and senior executive-level attention to critical security-related issues and the need for a comprehensive approach to protect the enterprise. The alliance members, ASIS International (ASIS) and ISACA, bring together almost 90,000 global security professionals with broad security backgrounds and skills to address the significant increase and complexity of security-related risks to international commerce from terrorism, cyberattacks, Internet viruses, theft, fraud, extortion and other threats.