

Booz | Allen | Hamilton

Convergence of Enterprise Security Organizations

November 8, 2005



Table of Contents

- 1.0 Executive Summary 1**
- 2.0 Introduction 2**
 - 2.1 Background..... 3
 - 2.2 Conditions for Convergence 4
 - 2.3 Project Scope..... 5
- 3.0 Findings 6**
 - 3.1 Imperatives Driving Convergence 6
 - 3.2 Implications 11
 - 3.2.1 Implications of the Rapid Expansion of the Enterprise Ecosystem 15
 - 3.2.2 Implications of Value Migration From Physical to Information-Based Assets 18
 - 3.2.3 Implications of New Protective Technologies Blurring Functional Boundaries 20
 - 3.2.4 Implications of New Compliance and Regulatory Regimes..... 23
 - 3.2.5 Implications of the Continuing Pressure to Reduce Cost 24
- 4.0 State of Convergence 25**
- 5.0 Conclusion 27**

1.0 Executive Summary

ASIS International identifies security “convergence” as a trend affecting global enterprises. ASIS International defines convergence as,

“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.”

—ASIS International

This definition captures a significant shift in emphasis from security as a purely functional activity within an enterprise, to security as a “value add” to the overall mission of business.

To gain a better understanding of the impact of convergence on global enterprises, the alliance of leading international security organizations including ASIS International, Information Systems Security Association (ISSA) and Information Systems Audit and Control Association (ISACA) retained Booz Allen Hamilton (Booz Allen) to examine this convergence trend within enterprises throughout the United States. Booz Allen solicited responses to web-based surveys on convergence from Chief Security Officers (CSO), Chief Information Security Officers (CISO) and other security professionals. Those security professionals interviewed and surveyed represent U.S.-based global companies with revenues ranging from \$1 billion to more than \$100 billion.

The overall high response rate among senior executives, who made up the majority of the interviewees, underscores the energy and importance behind this topic. The findings from the surveys and interviews point to several internal and external drivers, or “imperatives,” that are forcing convergence to emerge:

- Rapid expansion of the enterprise ecosystem
- Value migration from physical to information-based and intangible assets
- New protective technologies blurring functional boundaries
- New compliance and regulatory regimes
- Continuing pressure to reduce cost.

Study comprised U.S.-based global companies with revenues from \$1 billion to more than \$100 billion.

These imperatives are fundamentally altering the security landscape by forcing a change in the role security practitioners play across the value chain of the business. For example, as formal risk discussions become more integrated, cross-functional and pervasive, the expectation that physical and information security practitioners will generate joint solutions instead of independent views increases dramatically. The study identified a shift from the current state in which security practitioners focus on their function to a new state in which activities are integrated to improve the value of the business.

This new “business of security” requires security professionals to reexamine the key operating levers they have available to them. Although these operating levers (e.g., roles and responsibilities, risk management, leadership) are not new, the opportunity to use them in innovative ways may prove so. For example, the surveys and interviews presented clear evidence that as leaders in the business, security professionals need to move from a “command and control” people model to an empowering and enabling model, and develop an enterprise wide view of risk rather than an asset based view. Our analysis of the survey findings clearly shows convergence as a business trend with a great deal of momentum. Delivering on convergence is not just about organizational integration; rather, it is about integrating the security disciplines with the business’ mission to deliver shareholder value.

2.0 Introduction

As new technologies emerge and threats become increasingly complex and unpredictable, senior security executives recognize the need to merge security functions throughout the entire enterprise. A recent incident at the Sumitomo Mitsui Bank in London, England, in which hackers attempted to steal £220 million from the bank, underlines this principle. Even though the bank had strong information technology (IT) security measures in place, a physical security lapse occurred. Adversaries posing as janitors installed devices on computer keyboards that allowed them to obtain valuable login information.¹ This situation highlights and reinforces the need to bring together—in fact, converge—all components of an organization's security through an integrated and deliberate approach.

To be effective, this converged approach should reach across people, processes, and technology, and enable enterprises to prevent, detect, respond to, and recover from any type of security incident. Failure to adopt a unified approach to security can result in catastrophic consequences. In only three days in January 2004, the MyDoom e-mail virus caused roughly \$22.6 billion in damages as it spread to more than 200 countries.² In addition to the costs companies face to deal with the immediate effects of an incident, security incidents can cause more costly, long-term harm, such as damage to reputation and brand. Beyond the impact to Market Capitalization, if the issue threatens the public good, regulators may intervene, enacting stricter requirements to govern future business practices.

ASIS International understands the challenge associated with these types of enterprise-wide risks and recognizes that security functions within enterprises need to step up to the challenge. ASIS International describes this emerging phenomenon as convergence and defines it as,

“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.”

— ASIS International

ASIS International builds this definition on an understanding that the significant increase and complexity of security-related risks such as terrorism, cyber attacks, Internet viruses, theft, extortion, and fraud requires corporations to develop a more comprehensive approach to protecting the enterprise.

¹ Watson, James. “Physical and IT Security Must Go Together.” *Computing*, May 4, 2005.
<http://www.vnunet.com/computing/news/2071716/physical-security-together>

² Herman, Wendy. “Network Security—Trusted Communications.” Nortel Networks.
http://www.nortel.com/corporate/pressroom/feature_article/2004d/10_25_04_security.html

2.1 Background

The term “convergence” has a long and varied history. The term originates from the fields of science and mathematics. According to the *Oxford English Dictionary*, its earliest use can be traced to William Derham, an English scientist from the 17th and 18th centuries (best known for his effort to measure the speed of sound by timing the interval between the flash and roar of a cannon). Usage in the 19th century broadened, such as the coming together of fields of endeavor. In later years, people applied the term to wind currents, mathematical series, nonparallel lines, and evolutionary biology (Charles Darwin used the term in the 1866 edition of *The Origin of Species*).

By the middle of the 20th century, the term was also being applied to political science (i.e., convergence of U.S. and Soviet systems) and economics (i.e., convergence of national economies into a global economy). In the 1960s and 1970s, the development of computers and networks established the context for new meanings. Since then, the term has been applied to corporate strategies (i.e., merger of media giants Time Warner and AOL), technological developments (i.e., voice communications with data communications), evolutionary computing (i.e., means of modeling the tendency for genetic characteristics of populations to stabilize over time), and most recently the merging of security functions within business enterprises.

In today’s interconnected and global operating environment, it seems nearly impossible to follow developments in technology or business without encountering the word “convergence.” With a term as rich and diverse as this word, there is always concern that it will become simply another buzzword, thrown around with casual indifference in discussions, with participants using the same word to mean different things. If we are to think clearly about changes in the security world, we must understand these different meanings and their implications.

When used in the context of business, convergence means that nontraditional elements of a business are starting to be more alike, with units coming together to create competitive advantage. The increasing focus on security from an enterprise perspective has led to a new way of examining risks that institutions face as a whole. This, in turn, is leading to innovative approaches that emphasize integration—specifically, the integration of the risk side of business into the strategic planning side in a consistent and holistic manner.

In the past, management of the risk inherent in a business was a function embedded within the individual roles of the “C Suite.” The traditional approach was to treat individual risks separately and assign responsibility to an individual or small team. Managing a singular kind of risk became a distinct job, and performing that job well meant focusing exclusively on that one particular area. The problem with this stovepiped approach is that it not only ignores the interdependence of many business risks but also suboptimizes the financing of total risk for an enterprise.

Breaking stovepipes and addressing the suboptimizing of investments requires a new way of thinking about the problem. This new thinking brings together the various stakeholders in the problem set to work closely together. A major objective of this study is to understand how leading organizations bring together diverse elements and get them to orient on a common objective.

2.2 Conditions for Convergence

Because the concept of convergence is not unique to the security realm, we can examine other applications for insights regarding how to bring together diverse elements and orient them on a common objective. From these past lessons, it becomes clear that convergence has one very important condition: a common framework from which to operate. Obviously, many “common framework” choices exist and in recent years, we have seen many attempts to implement a variety of structures.

The study identified that a common first choice focused on an organizational option. An obvious, and flawed option, is to consolidate the disparate functions under the strongest or most powerful of the various security elements. The rather predictable result is a decline in the influence of the elements that have been imported. Another approach is to move all of the security elements into a “non-affected” element of the business (e.g., Human Resources). This organizational construct may serve to minimize the chances of the non-affected element eclipsing the imported elements, but it often creates other tensions concerning the planning and execution of functional responsibilities.

There are limits to how far an organizational solution can be applied in setting the conditions for security convergence. Of particular concern is the structure’s long-term viability. If the organizational structure does not support the overall business goals, then it is unlikely to sustain over time.

A powerful approach identified in this study, outlines a business-focused “council” of leaders approach. The business-focused framework calls for each security element to come together using the corporate strategy as a common element on which to focus. This approach requires all stakeholders in the security realm to use a common language: the language of the business units. It sidesteps any thorny issues associated with organizational changes alone by shifting emphasis from “*For whom do I work?*” to “*What am I doing for the business?*”

The ASIS International definition captures this shift to the business framework by emphasizing language like “the identification of security risks and interdependencies between business functions and processes” and “managed business process solutions to address those risks and interdependencies.” This change in emphasis should have a profound impact on how business unit leaders view security. Indeed, it sets the conditions to allow convergence to emerge.

2.3 Project Scope

Those security professionals interviewed and surveyed represent U.S.-based global companies with revenues ranging from \$1 billion to more than \$100 billion. A majority of security professionals oversee organizations with more than 50 employees, and budgets exceeding \$10 million. The participating entities represent a wide variety of industries (e.g., financial services, pharmaceuticals, biotechnology, automotive, telecommunications and technology, utilities, healthcare), and have global operations, on average, in over 40 countries throughout the world.

There is considerable interest in the subject of convergence, as demonstrated by the high response rate among senior executives who made up the majority of the interviewees. During a three week span in August, more than 50 percent of those solicited for the surveys responded (36 out of 70 companies replied). Booz Allen also conducted 14 interviews out of 25 solicitations, in which the majority of the participants were the most senior security professionals in the organizations. The companies interviewed were responsive, accommodating, and had definitive viewpoints.

3.0 Findings

The results of the survey and the conversations in the interviews reinforced the impression that security convergence is a present phenomenon that is making a significant impact across enterprises in all industries. Furthermore, the study identified several new internal and external drivers, or imperatives, in the current operating environment. These imperatives are creating the conditions that allow security convergence to emerge as an operating norm.

3.1 Imperatives Driving Convergence

Five distinct imperatives are driving security convergence and will continue to affect companies across sectors and geographies: (1) rapid expansion of the enterprise ecosystem; (2) value migration from physical to information-based and intangible assets; (3) new protective technologies blurring functional boundaries; (4) new compliance and regulatory regimes; and (5) continuing pressure to reduce cost. Table 1 describes the five imperatives.

Table 1. Description of Imperatives

Imperatives	
Rapid Expansion of the Enterprise Ecosystem	Enterprises are becoming more complex in a global economy where external partners are increasing (i.e. outsourcing)
Value Migration from the Physical to Information-based and Intangible Assets	Increasingly, value is shifting from physical to information-based assets
New Protective Technologies Blurring Functional Boundaries	Emerging technology is creating an overlap between physical and information security functions
New Compliance and Regulatory Regimes	More regulations are developing in response to new threats and business interactions
Continuing Pressure to Reduce Cost	Enterprises are constantly trying to efficiently mitigate risk

Rapid Expansion of the Enterprise Ecosystem

The enterprise ecosystem³ is rapidly expanding as businesses implement new technology and practices, creating more complex organizational structures. For example, as many companies turn to third-parties to reduce cost by outsourcing, they are adding another organizational layer. About 73 percent of North American companies outsource some IT function,⁴ creating external business partners globally. Enterprises must now consider the integrated security implications of outsourcing specific functions to other companies and managing alliances to create competitive advantage.

Value Migration from Physical to Information-based and Intangible Assets

Companies' assets are now increasingly information-based and intangible. Even most physical assets rely heavily on information. For example, manufacturers are dependent on receiving specific information from suppliers before the process of producing the physical products can commence. The security of this information is vital to the development of physical products. Technology is also now allowing companies to offer more information products. News service and research companies, for example, provide nothing but information to their customers. They must ensure security of information not only to their customers but also from their suppliers. As these assets become increasingly intangible, there is a greater need to integrate physical and information security, as well as security throughout the entire enterprise.

New Protective Technologies Blurring Functional Boundaries

New security needs are blurring functional boundaries inside an organization. For example physical access control technology is now merging with network access technology, requiring physical and information security groups to integrate their strategies. The *smart card* is an example of a technology that is integrating once disparate parts of security, by verifying a person's identity and tracking his or her physical location.

New Compliance and Regulatory Regimes

As new threats emerge and business transactions become more intricate, it follows that adherence to regulations and compliance guidelines will become more complex. For example, Sarbanes-Oxley gives a framework under which risk must be assessed, but falls short of mandating how to assess that risk. These laws only serve as a baseline for security professionals requiring minimum levels to be met. The complexity results in the managers' ability to be forward sensing when assessing an enterprise's security needs.

³ For the purposes of this study, an ecosystem is a dynamic and complex business entity, with individual elements interacting together, but overall acting as a single unit.

⁴ Sharma, Sunil. "IT Outsourcing Trends and Opportunities." November 5, 2004.
<http://www.gantthead.com/article.cfm?ID=221004>

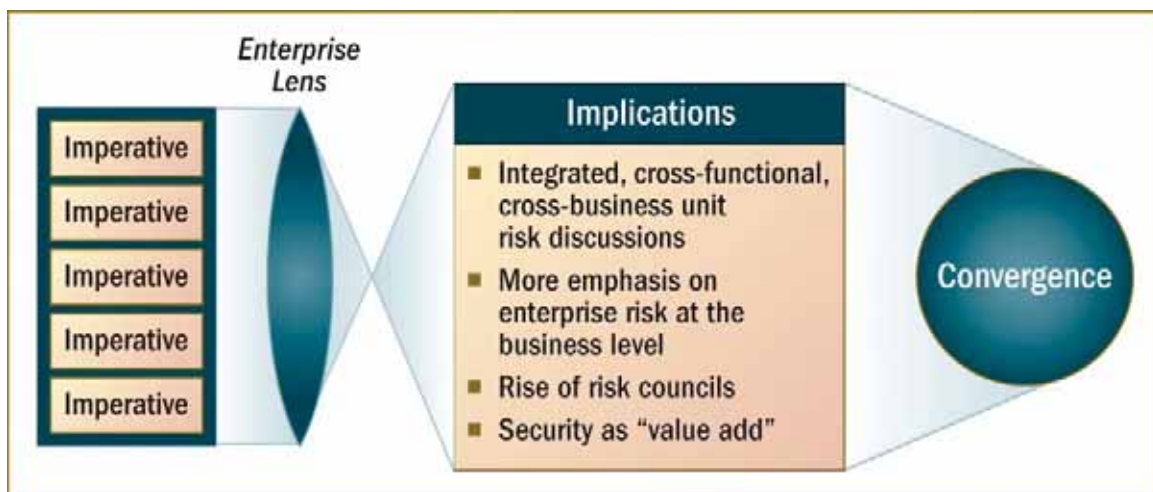
Continuing Pressure to Reduce Cost

Finally, enterprises will always grapple with balancing risk/reward tradeoffs. As risks become increasingly complex, enterprises must take a systematic, pragmatic approach to security that maximizes resources while adequately managing risk. In an era of rapidly changing risks, efficient allocation of security resources requires a risk based approach and greater transparency related to security strategy. What we will and will not focus on needs to be clear to avoid continual realignment based on the most “recent” set of issues, versus the most important.

Fundamentally, these imperatives are forcing changes across the entire value chain of the business, while also changing the role of security within an organization. There is an increased perspective on enterprise risk at the business level, with the emergence of risk councils. In addition, security is progressively being viewed as a “value add” and even a competitive advantage for numerous enterprises.

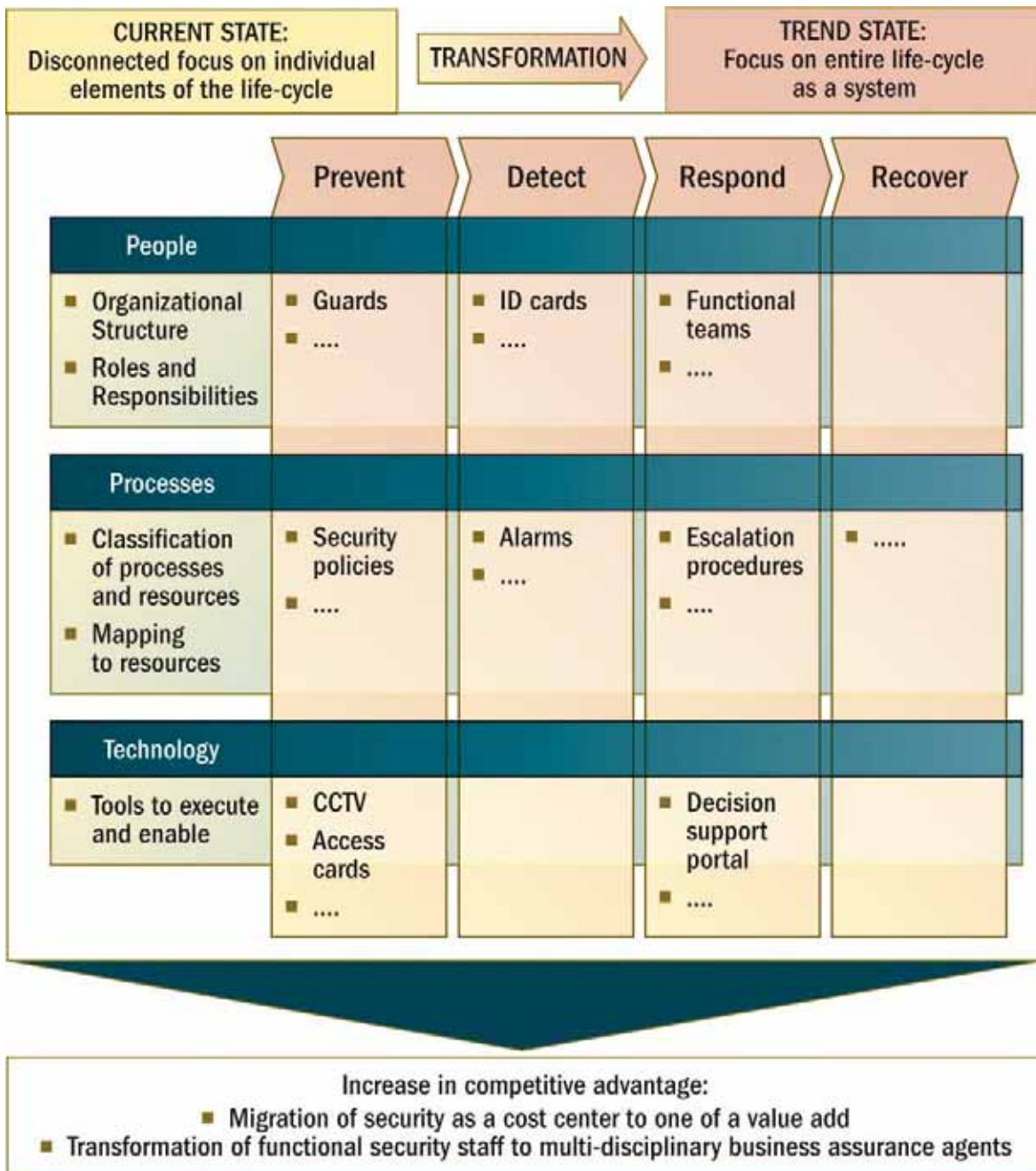
These imperatives and their implications are driving organizations toward security convergence as outlined in Figure 1 below.

Figure 1. Imperatives and Implications Driving Security Convergence



Security convergence is pushing companies to focus beyond functional dimensions to include all parts of the security and business life-cycle, creating a need for a unified security framework (see Figure 2). The study indicated that the framework for converged security must incorporate people, processes, and strategies. It must enable an enterprise to prevent, detect, respond to, and recover from a security incident. Furthermore, the survey and interviews showed that enterprises are realizing the need to move away from a disconnected focus on individual functions and elements of the security life-cycle (i.e., prevent, detect, respond, recover) to focus on the entire business life-cycle as a system. Appreciation of this transformation can significantly increase an organization's competitive advantage: two prominent examples center around cost and people leverages. Cost advantages can be realized through the migration of security as a cost center to one of a value add – reducing costs, providing of cost efficiencies, and achieving certain cost avoidances. People advantages can in turn be realized through the transformation of narrowly focused functional security staff to broad based multi-disciplinary business assurance agents – with exponentially increased impact over the mere summation of the individuals.

Figure 2. Life-Cycle and Functional Dimension of Security Convergence



Many physical and information security components currently focus on only one part of the security life-cycle. For example, many security organizations concentrate most of their efforts on their ability to respond to a security incident. In the pharmaceutical industry, for instance, this reactive mode has resulted in increasing the overall risk level. According to the Financial Times and based on a study by KPMG, investing in the pharmaceutical industry carries 50 percent more risks than in the overall S&P 500, because big Pharma's management of operational risks has lagged behind dramatic and reputational shifts and drug makers must change their risk management processes from thinking in terms of compliance to thinking in terms of risk prevention.⁵

One security professional indicated that, "standards for one area that have strong requirements from another area are driving the need to take a business approach to risk management."

⁵ FT Companies & Markets. "Big pharma needs to overhaul risk assessment," week 38, September 19, 2005, page 17. Copyright, The Financial Times Limited 2005.

3.2 Implications

Study participants outlined that successfully integrating the multiple facets of a converged security program can help stem many of the negative implications brought on by market and environmental factors. Companies use a range of formal and informal mechanisms to accomplish their mission. In the course of the study, we identified a set of nine commonly used operating levers used to effect change and execute against the firm's mission as outlined in Table 2 below:

Table 2. Operating Levers Existing within Organizations

Operating Lever	Description
Risk Management	Evaluating threats, vulnerabilities, and business impacts to determine strategy for operating within an acceptable level of risk
Governance	System and processes in place to establish authority and responsibility
Budget Processes	Method by which all of the anticipated expenses and revenues of an enterprise are determined
Standards & Guidelines	Documentation that establishes the parameters for process to be implemented within an organization
Integration	The fusion of functions and processes between different components of the enterprise
Business Case	Structured document describing an analysis of the situation and an intended course of action for success
Roles and Responsibilities	Formal documentation of the responsibilities within each role of an organization
Leadership	The authority to guide or direct the actions of a company
Knowledge of the Business	Understanding of the enterprise's mission, goals, objectives, and its organization

In many companies, security leaders apply these levers individually rather than woven together to arrive at a cohesive approach to securing the organization's assets and ensure mission success. Often, practitioners react to their specific operating environment by establishing individual stovepiped solutions to manage a respective operating lever. This disjointed approach lends itself to poor communication and redundant or counterproductive security controls implementation. At some level, organizations implement these specific levers to determine a variety of business and security decisions. These nine levers break into three distinct categories: **strategy, process, and people.**

Strategy levers include risk management and governance. Most companies have a risk management group that is responsible for assessing risk and then supervising those threats through effective strategies. These strategies usually include transference, avoidance, mitigation, and acceptance. Enterprises should shift their risk management view from one based primarily on only protecting assets to one that takes into account the security of the entire enterprise. Governance refers to the way in which its leaders manage the enterprise. To facilitate security convergence, a governance structure should move from a passive and infrequent environment to one that has active board involvement so leaders can drive convergence throughout the enterprise.

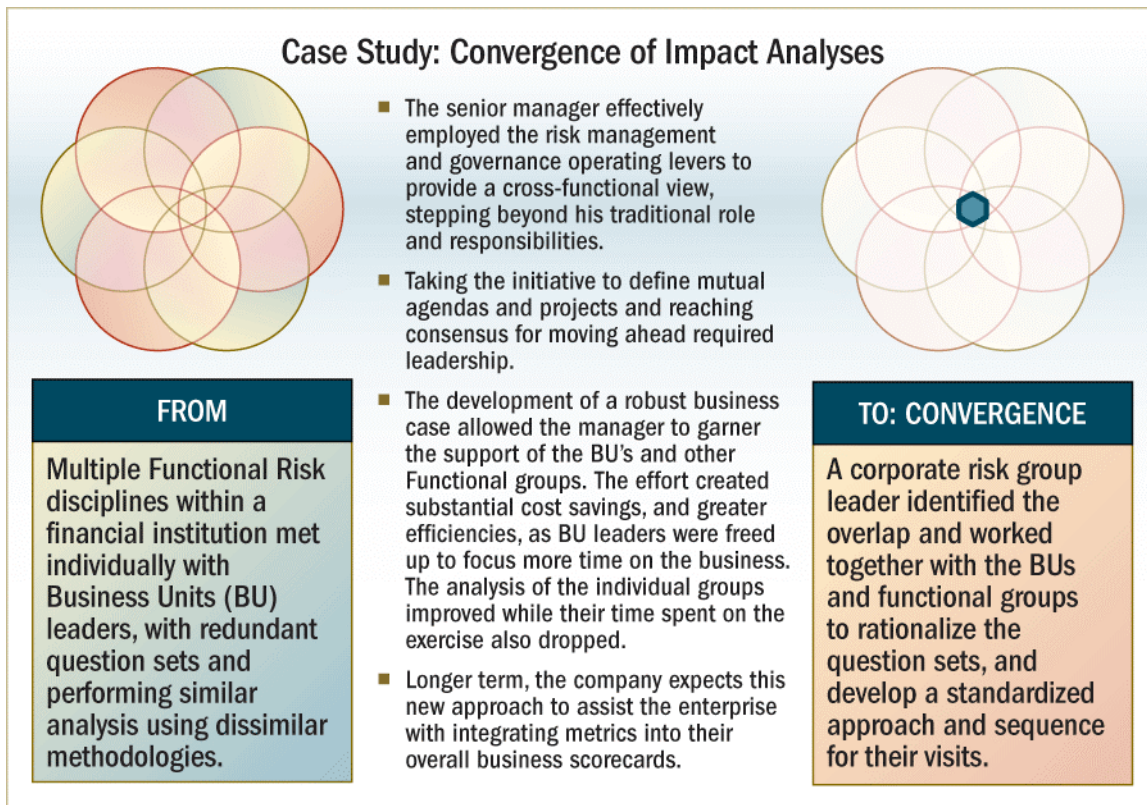
Process levers include such areas as budget processes, standards and guidelines, integration, and the business case. While these business-based processes are not solely with the typical security domain, they are valuable tools in managing security convergence. Security elements within the business should become masters of the budget process, understand fully applicable standards and guidelines, and embrace the business case as the common language to discuss investments with peers. Standards and guidelines are policies that direct internal processes and procedures, and are critical for a comprehensive approach to attain business goals. Therefore, enterprise standards and guidelines should not be functionally focused, but rather common and shared widely.

In addition, integration, which refers to the fusion of functions and processes between different components of the enterprise, should not be forced, but adaptive to the constantly changing environment. Emerging technologies often characterize this kind of environment. As new technologies and new risks emerge, different components should respond to new security measures using various methods of integration. Employees are not receptive to forced integration but will be more agreeable if they perceive its benefits to the entire enterprise. Therefore, security organizations should move from not using a business case or using a business case that is highly technical, to making it “C Suite” language. The business case describes the need that a project will meet, written in a form that is clear to senior-level executives. To embed security throughout an enterprise, those who are not directly involved with security must perceive its value in a clear business case.

The **people lever** consists of exhibiting leadership, defining roles and responsibilities, and building a core knowledge of the business across the organization. While the command and control may be necessary during crisis, an empowering and teaching mode is needed to build more “leaders” across the business. In addition, the proper documentation of an individual’s role and responsibilities within that position foster job performance at that level and identify the capabilities required at the next level. A capability maturity model for security professionals is considered a crucial element of a long-term strategy to deal with the distributed challenges of managing security across a global footprint. Leaders have a responsibility to broaden the competencies within each role across the “converged” footprint. Providing timely and accurate information about performance while fostering the connectedness of staff in a consistent manner is crucial to the success of a converged security initiative. Employee retention and productivity link directly to shared expectations and a common understanding of the goals for the company.

A change in approach, from narrow and focused, to holistic, helped the firm noted in Figure 3 achieve a unified security framework. The operating levers it employed were not new, but the manner in which they were applied required adapting and applying them in a unique context to create value. Creating a common view of mission across disparate risk domains yields substantial value.

Figure 3. Case Study: Convergence of Impact Analyses



As exemplified above, study participants indicated a substantial shift in their approach to these operating levers as noted in Figure 4 below:

Figure 4. Shift in Operating Levers

Operating Levers		From	To
Strategic	Risk Management	Asset-based view	Enterprise-wide view
	Governance	Passive and infrequent	Active Board involvement
Process	Budget Processes	“Not my domain”	Common language with peers
	Standards & Guidelines	Functionally focused	Common and shared widely
	Integration	Forced	Adaptive
	Business Case	Technical/jargon-filled or none	“C Suite” language
People	Roles & Responsibilities	Functionally defined	Multiple competencies
	Leadership	Command and control	Empowering and enabling
	Knowledge of the Business	Functional expertise	Broad business understanding

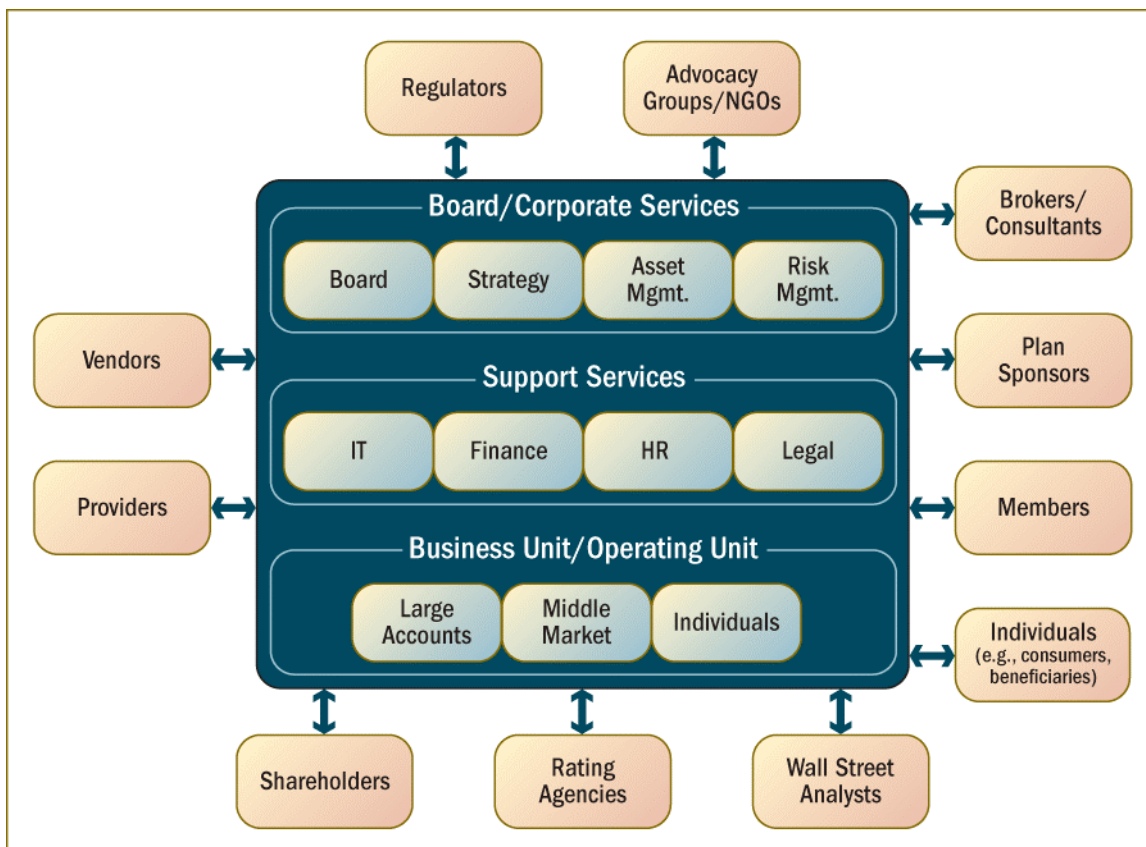
Applying a security convergence strategy with respect to these operating levers can generate positive returns for any organization. Adapting the way in which traditional operating levers are used will help enterprises realize immediate and long-term benefits of security convergence. In addition, the pace of change within the operating environment has significantly increased over the past decade with company leadership facing new realities. These realities are driven by business, competition, threats (natural and man-made), industry, legislation, and emerging technologies.

During this study, we developed examples for each of the major levers against the imperatives driving change in most organizations. The levers called out in each were identified as having the greatest impact on that respective imperative. Today’s operating environment is a dynamic one. Internal and external drivers, or imperatives, are continually present and illustrate the importance of the levers.

3.2.1 Implications of the Rapid Expansion of the Enterprise Ecosystem

In today’s global economy, outsourcing and emerging technology are creating more interconnected environments, expanding the enterprise ecosystem into a much larger, complex system. Organizations are increasingly relying on external partners as integral components in daily business. For example, manufacturers rely on just-in-time supplies arranged by a complex network built on information sharing with suppliers and vendors, infrastructure stability, and regulatory compliance, as shown in Figure 5.

Figure 5. Multiple External Partners Affect Business Outcomes



Disrupting information and supplies, interrupting transportation mechanisms, or failing to meet certain compliance requirements, can lead to the dislocation of an entire product line. Consider what happened in September 2002 when a labor dispute shut down west coast ports for several weeks. As critical supply chains stopped functioning normally, severely constraining manufacturing and product replenishment, U.S. companies lost an estimated \$1 billion per day. The events highlighted the interdependencies among shipping companies, supply chain-intensive industries, contract logistics providers, and government agencies. One company that produces information products indicated that its decision to establish an “external security chain of trust” came as a result of its reliance on information from other suppliers. Situations such as these demonstrate the need for developing positive relationships with external partners. Starting from a positive position can help improve the understanding of the interdependencies between the parties and help each company better plan for discontinuities that might occur within the system.

The rapid expansion of the enterprise ecosystem also requires that enterprises establish relationships with the public sector. Government partners are also essential external stakeholders, especially for those companies that own or operate the nation’s critical infrastructures. One example is The Infrastructure Security Partnership (TISP), a forum for U.S.-based public and private sector nonprofit organizations to collaborate on issues related to the security of the nation’s critical infrastructures. TISP acts as a national asset facilitating dialogue on physical infrastructure security, by leveraging members’ technical expertise, and research and development capabilities in the design and construction industries. Members include U.S.-based federal, state, and local agencies; professional associations and industry trade groups; codes and standards organizations; universities; and infrastructure developers, owners, operators, and service providers whose main purpose is related to the design and construction of the nation’s built environment. TISP’s objective is to create a collaborative environment that will raise awareness and lead to sustainable security improvements to the U.S.-critical infrastructure. TISP is working to arrive at mutually agreeable information sharing processes for protecting these infrastructures.

Defining the extended enterprise is a first step toward developing a consolidated view of risks. Risk management plans can be developed to identify gaps and prioritize risk management objectives, reaching across the extended ecosystem and engaging partners in the process. Enterprises should build a trusted information-sharing relationship with the important, public and private sector constituents engaged in their system. This system of trust and information sharing will support all entities in controlling risk. In addition, selecting trusted security suppliers helps coordinate prevention and response capabilities with public and private sector partners.

Ways to Facilitate Convergence

- Build a trusted information sharing relationship
- Establish uniform security language in contracts
- Develop staff with knowledge of external stakeholders

For example, one interviewee noted that business continuity functions in leading organizations are now reaching beyond the organizational boundary to drive the sharing of information and development of memorandums of understanding with critical suppliers, customers, and local first responders. Federal clients are also extending continuity of operations planning to share risk information, strategies for minimizing risk, and sharing response resources to streamline costs.

Benefits

- Better collaboration
- Enhanced ability to select secure suppliers
- Coordinated prevention and response capabilities
- Increased visibility into supply chain security
- Maintain control in a rapidly devolving environment

Leaders should establish uniform security language in contracts using standards and guidelines. Establishing a common language, readily understood by external partners, creates the foundation for a unified approach to security. This common language helps an enterprise maintain risk control in a rapidly devolving environment. For example, companies are realizing that it is often easier to establish a secure “extended network” across international boundaries using contracts that reference standards than waiting for various national standards and international agreements to mandate these same standards.

The recent establishment of the National Incident Management System (NIMS) is an attempt at establishing a standard approach for the myriad of responders involved in emergency response. NIMS integrates effective practices in emergency preparedness and response into a comprehensive national framework for incident management. The benefits of NIMS will be significant, including standardizing organizational structures, processes, and procedures; establishing interoperable communication processes, procedures, and systems; and acquiring equipment acquisition and certification standards. NIMS will create a convergence of responders at all levels, enabling them to work together more effectively to manage domestic incidents regardless of cause, size, or complexity.

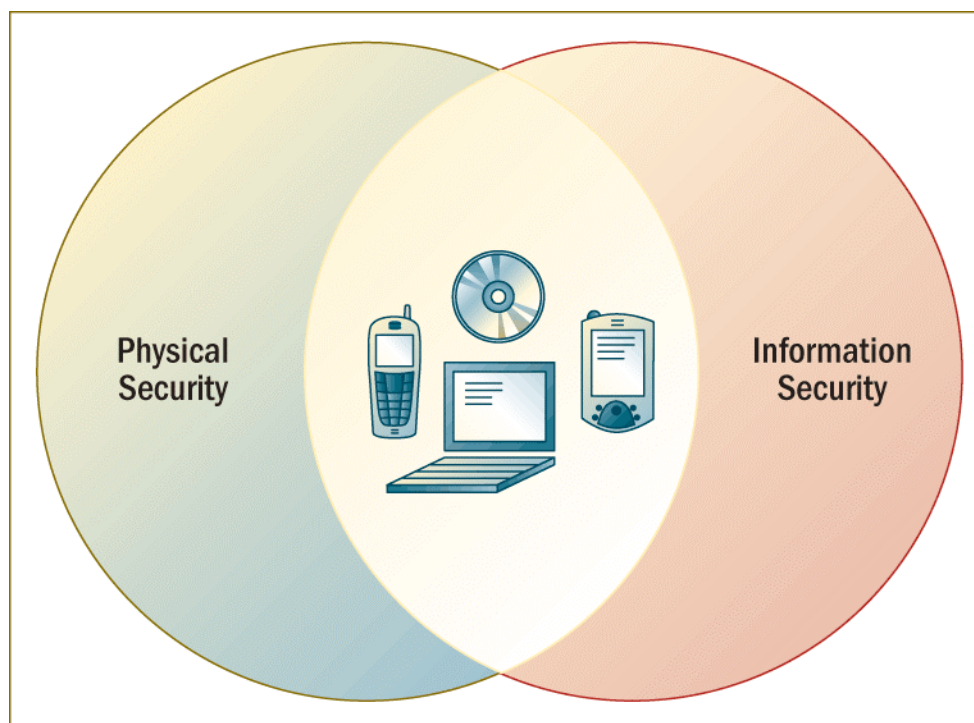
In regards to roles and responsibilities, security professionals must continue to develop staff with knowledge of external stakeholders to serve as liaisons with the extended enterprise. This effort will increase the visibility into supply chain security, enabling an organization to identify and plan for potential problems. Ultimately, expanding the scope of understanding required of security personnel will help security professionals to contribute more effectively to the bottom line; engage more meaningfully with external stakeholders; anticipate challenges or potential problems; and recommend strategies to mitigate, respond to, or recover from a crisis.

For example, to protect a high value product line better, a security organization might hire an engineer who understands what is required of a supplier to create and produce the products.

3.2.2 Implications of Value Migration From Physical to Information-Based Assets

Information is increasingly a product of physical assets, requiring greater integration of physical and information security (see Figure 6). For example, increasing cooperation exists between investigations and computer forensics as a result of merging physical and information security efforts. Furthermore, more physical security standards now exist for information assets that are requiring the two groups to merge. One company indicated that individual identity records are worth \$60 on the black market, and one backup tape full of these records can be worth more than \$1 million. Enterprises must ensure that this information is physically secure. This is possible only if physical and information security reaches across their functional domains to work together with the goals of the business in mind.

Figure 6. Information-Based Assets



In this case risk management requires facilitation of security convergence. Enterprises must understand that information assets are often a product of multiple process owners. Security leaders must therefore manage risks to information across the enterprise. Organizations that can identify “white space” risks that exist between traditional disciplines or do not appear until a project is well under way can help create transparency and more comprehensive risk prioritization. An example of a white space event is a typical “smash and grab” theft of laptops that contain important employee information. An example of this situation and its mitigation impact across multiple domains was offered by a participant—a security guard who is improperly trained in bomb threat protocols, acting on a nonspecific threat, discards a piece of IT equipment without recognizing the IT implications of such an action.

As physical and information security domains are working more closely together, it is important to understand other groups' roles and responsibilities within an enterprise to advance physical and information skill sets. Merging physical and information security forces has been shown to reduce costs and allow adaptability to emerging information protection needs. For example, one company noted that its physical security investigative team joined with the computer forensics team to reduce computer abuse, which resulted in a 25 percent increase in available bandwidth and reduced full time equivalents needed to manage this risk.

Ways to Facilitate Convergence

- Identify “white space” risks between traditional disciplines
- Develop an understanding of other groups' roles and responsibilities
- Understand business value drivers

Benefits

- Understand and mitigate submerged risks
- More comprehensive risk prioritization
- Greater alignment of priorities
- Increased ability to adapt to emerging trends
- Better alignment with business goals

Security personnel who understand physical and information security can evaluate a wider view of risks and vulnerabilities and determine the most effective (and cost effective) method of mitigation, including reinforcing the selected approach with other options, both information or security related. For example, when a federal government agency evaluated risks to its organization through an enterprise-focused impact analysis (rather than stovepiped department-focused), it identified several single points of failure resulting from no single discipline realizing complete ownership of the issue. Through enterprise-focused discussions with a unified information and physical security branch, the agency was able to determine an information security approach to mitigate one of the issues and reinforce the approach with physical security measures.

An understanding of the business value drivers is essential for security convergence. This understanding helps enterprises focus on strategic initiatives and creates greater alignment with business goals, strategies, and objectives. Companies need to look no further than the variation between business continuity goals and IT contingency plan capabilities to see that most often, IT systems lack the design elements to meet business recovery time objectives based solely on a lack of communication or understanding between the two. To attain security convergence, one company reported that it developed a “security professional” career path through which it rotates people in physical, information, business unit, and corporate functions to attain a comprehensive ability to understand and operate across all domains. Another approach considered by a federal government agency was to cross-train those responsible for business continuity and IT recovery planning. This approach provided a deeper understanding of the business on both sides and alternate methods for responding to emergency events.

“A hit to reputation can cost a company several hundred millions compared to a few million even from a significant loss of assets.”

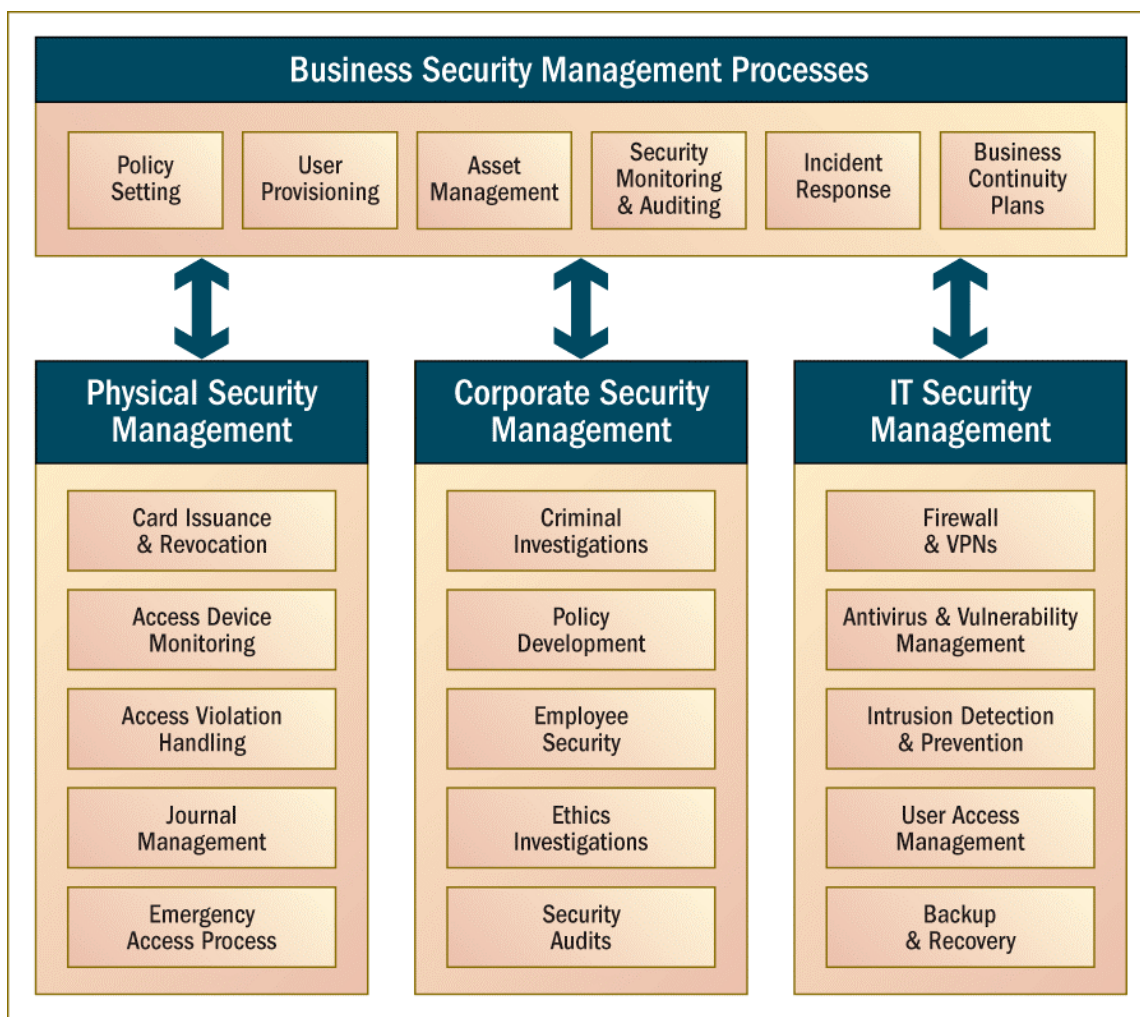
3.2.3 Implications of New Protective Technologies Blurring Functional Boundaries

New and emerging technologies designed to improve physical and information security are making functional boundaries less discrete, forcing security organizations to work together to realize business goals. As an example, one company described a situation in which they successfully combined their efforts around a protective technology that affected both physical and information security. Physical security was seeking to standardize door access badges, but information security was developing virtual private network (VPN) access cards. The two groups discovered each other's efforts through collaboration on the business process layer and worked together to conduct common risk analysis and return on investment (ROI) justification for combining projects. This effort resulted in collaboration on the project closeout to show realized ROI.

Increasingly, assets, whether physical or information-based, have physical and information security related risks. As illustrated in Figure 7, converging the security management process into a *Business Security Management Process*⁶ moves the traditional physical security management or IT security management into an approach with a wider spectrum with which to plan for, monitor, and respond to vulnerabilities. This unified entity then has the capability to understand the enterprise in its entirety rather than have access to only elements pertaining to specific information or physical security concerns. Consequently, a Business Value driven organizational approach that lends itself to physical and technical integration was viewed as optimal for this entity.

⁶ This includes policy setting, user provisioning, asset management, security monitoring and auditing, incident response, and business continuity plans

Figure 7. Business Security Management Processes⁷



To facilitate security convergence caused by the blurring of functional boundaries, enterprises are learning to cooperate across functional domains by leveraging the budget process. Security organizations should understand the budget process and reach out to others to determine common projects and risks to better leverage the resources for mutual efforts. This will provide an ability to escalate relevant projects and will bring competitive advantages through enhanced productivity. One security professional indicated that he had, “directed [his] staff to learn the budget process. This resulted in greater cooperation with Finance and IT.”

Ways to Facilitate Convergence
<ul style="list-style-type: none"> ■ Cooperate through budget processes ■ Integrate and share initiatives ■ Reach out across functional boundaries

⁷ “Enabling Comprehensive Security Management.” Open Security Exchange. http://www.opensecurityexchange.org/info/ose_brochure.pdf

Benefits

- Ability to escalate relevant projects
- Competitive advantages through enhanced productivity
- Improved capital allocation
- Cost reduction
- Collaboration and interoperability

Companies should integrate risk agendas into shared initiatives, which focus these initiatives on managing the risk of the organization rather than managing only the individual functional areas. This, in turn, will improve capital allocation through combined risk prioritization. Physical and information security should merge to create a model for efficiency and management of resources for the benefit of the organization. Integrating security into every aspect of the business can reduce risk. By prioritizing risks from an enterprise viewpoint, rather than prioritized within each discipline, organizations are able to allocate funds to the most critical risks while also identifying projects that mutually benefit multiple disciplines. By resolving vulnerabilities from an enterprise approach, organizations

can mitigate a vulnerability existing in one discipline, which consequently reduces downstream risk to another.

Integration of *Business Security Management* (see Figure 7) should follow the system life-cycle approach. Security of the information or physical asset is built into product design at the initiation stage and carried through development/acquisition, implementation, operation/maintenance, and disposal/transition phases of the product. Each review and modification to the asset brings the *Business Security Management* together with the product team to provide input on security modifications and approaches thus making security of the product inherit in its design and application.

It is critical to develop relationships with people across functional boundaries to facilitate security convergence. Security leaders should proactively reach across functional boundaries to discover mutual projects. This action will help to reduce costs attributed to the mitigation of duplicative efforts and will increase interoperability of security functions. One company builds relationships by holding executive coffee events three times a week. These events have helped develop executive-level outreach and security management buy-in. Furthermore, they are now a “hugely successful part of the corporate DNA” and have greatly aided security convergence. Senior management buy-in of business security is essential to promoting staff to follow through on implementing security measures and funding allocation. Because ROI of business security can be difficult to quantify, a broad understanding of the importance throughout the organization can often qualify the investment.

For example, one company does not launch a product unless a member of the physical security team is on board.

A converged security organization that is aware of projects across the enterprise is more likely to find similarities in work and mitigations. One senior manager in the corporate risk group at a financial institution discovered that six different functional groups within his enterprise were conducting their own impact analysis of various assets using different question sets and separate resources. He took the initiative to rationalize the question sets and develop a standardized approach to financial analysis. This was a way to create common processes.

A security professional simply suggested, “Go have a beer with your colleague.”

3.2.4 Implications of New Compliance and Regulatory Regimes

In an increasingly complex regulatory environment, companies must balance their focus on compliance. One security professional stated, “Mere compliance to stay out of jail is of no real use to the company or people.” On the other hand, if there is undue focus on compliance, an enterprise can create a distortion of risk priorities and agendas, a false sense of security, and a warped asset allocation. Another security professional warned that this could create a “warping of priorities into an economic fiction, driven by regulation that does not serve well in the marketplace.” Effectively leveraging compliance can result in optimal risk posture when the following exist: a business strategy driven risk agenda, appropriate levels of accountability, an embedding of compliance and audit processes, and guidelines rather than standards.

3.2.5 Implications of the Continuing Pressure to Reduce Cost

Ways to Facilitate Convergence

- Migrate from insurance focused to enterprise-wide view
- Help develop active Board awareness and involvement
- Develop shared common processes focused on the business

Organizations, regardless of industry, generally strive to reduce costs in every facet of internal operations. Security has always been a visible target for cost reduction because it is not viewed as revenue producing and there is difficulty in demonstrating ROI.

A dashboard view of combined risk priorities helps create transparency and accountability. Leaders in the security arena should prioritize all risks, regardless of type, so that the enterprise can focus spending on critical risks, thereby optimizing investments and reducing inefficiency. An information security risk may have physical security ramifications and vice versa. A

comprehensive look at all identified risks can assist in determining mitigation strategies. A converged solution may at times cost more to develop, but ultimately mitigate more than one risk and have a longer shelf life, thus reducing overall expenditures.

Enterprise Security Organizations should streamline and simplify their budget requests, using a common language in order to help facilitate security convergence. This cross-functional integrated approach ensures assessment of all aspects of spending are consistent with security as well as business objectives. To do this, senior security staff must become more proficient at navigating the budget process. One company interview achieved this by integrating their security budget and program goals into their firm's overall "resource planning tool" process—with very positive results.

Communication between and among departments is critical within the budget process. A proposed solution within the Office of the Chief Information Officer (OCIO) may mean added cost for the Office of the CSO (OCSO), or vice versa. For example, a switch to a new operating system for network servers may mean added security for electronic information but may result in a costly retrofit for the company's access control software. Emerging physical security technologies rely heavily on IT resources and any changes within the OCIO will affect physical security controls.

"The goal is not a static picture of minimized risk, but the maintenance of certain risk issues within an acceptable variance."

Organizations should establish clear ROI hurdles by conducting careful risk analysis and establishing spending guidelines to bring about security convergence within an enterprise. Initially, companies should strictly identify and establish their strategic direction and goals, creating transparency about what is in scope/out of scope. This business case will ensure that all activities undertaken support mission accomplishment. Failure to adequately plan for and document the business case often results in wasteful spending. Reaction to "pop-ups" can drain the energy and funding of a security organizations. The business case will help align resources with priorities and bring competitive advantage through better capital management. One security professional agreed with the need to prioritize risk when he stated, "The goal is not a static picture of minimized risk, but the maintenance of certain risk issues within an acceptable variance." A business case is an important tool for documenting acceptable risk levels and ensuring that proposed security controls do not interfere with the operation of the company. Components of an organization must share vulnerabilities and not be afraid to expose weakness to begin the process of reallocating funds to the most critical problems. This effort will create a culture of collaboration in which everyone is working together toward a common goal.

4.0 State of Convergence

The public and private sectors, realizing that security convergence is necessary in the current dynamic environment, are investing resources to integrate security. The security convergence market is rapidly growing. In 2005, the private sector in North America and Europe is expected to spend more than \$300 million on convergence efforts, while combined, the public and private sector spending is expected to exceed \$1.1 billion in 2005.⁸ Table 3 shows a forecast of security convergence spending in Europe and North America.

Table 3. Forecast: Europe and North America (NA) Security Convergence Spending

	2004	2005	2006	2007	2008
Large-scale convergence projects in NA and Europe	19	68	175	382	856
Physical/logical access control projects in NA and Europe	50	150	413	903	1,656
Other projects performed jointly by IT and physical security departments in NA and Europe	13	45	118	246	406
Public sector: border control convergence systems, law enforcement projects in NA and Europe	410	820	1,899	4,202	8,003
Small projects (data center security, communications security, etc.) in NA and Europe	14	40	108	229	369
Total	506	1,123	2,713	5,962	11,289

As spending increases to support security convergence efforts, addressing underlying barriers to convergence also should be a priority. Survey results showed that a significant percentage of respondents believed there was not only a tendency for assurance capabilities to be viewed as operational functions rather than strategic imperatives but also a fragmentation of risk management activities, which hindered unification of the risk management approach. Both findings underscore the need to increase organizational awareness and buy-in for the cross-functional relationship of security throughout an enterprise and its extended ecosystem.

Findings also indicate a potential disconnect among board member priorities, where it is judged to be “not on the radar” and security priorities, where it is a top ten priority for more than half. For security convergence to be realized, it must become a priority at the board level ensuring adequate ...convergence is a high priority for more than half of survey participants, but it is not judged to be “on the radar” for more than half of the boards.

⁸ Hunt, Steven. “Trends 2005: Security Convergence Gets Real.” Forrester Research. January 11, 2005. http://www.opensecurityexchange.org/downloads/forrester_trends_2005_convergence.html

The establishment of security convergence should involve not only those routinely responsible for security (e.g., Chief Financial Officer, Chief Information Officer, and CSO) but also the Chief Executive Officer, business unit general managers, board of directors, and board's audit committee. Security leaders must advocate convergence throughout the organization and collaborate with all organization members, using bottom-up and top-down approaches. Looking beyond organizational boundaries, engaging business partners in the security discussion is also a requirement in today's global economy.

As security staff whittles down these barriers to success, and personnel are able to influence the way in which operating levers are used, enterprises will realize the impact of security convergence. They will see this evolution through an increased ability to adapt to meet changing security needs, greater alignment of business goals, strategies, and objectives, and seamless external coordination. Overall, the entire business system benefits from security convergence.

5.0 Conclusion

The convergence of security within enterprises is rapidly emerging. Enterprises need to recognize this emergence and begin to adapt accordingly. As discussed in Section 2.2, “Conditions for Convergence,” various common frameworks exist from which to operate and create conditions for convergence. However, it is clear that a business-focused framework will allow security elements to become part of the strategic landscape of the enterprise, thus legitimizing security as a critical element of the enterprise. The role of security in the enterprise is no longer seen as a sunk cost but a value adding activity.

This business-focused framework further enables an integrated, unified approach to security that reaches across people, processes, and technology, and focuses on the entire business life-cycle as a system. As Christopher Kelly, a Vice President at Booz Allen, stated at the ASIS International Annual Conference 2005,⁹ “Convergence is requiring our security leaders to learn much more about the business and change their perspective of their position, from a functional subject matter expert to a business person with functional knowledge.”

As security convergence continues to emerge within an enterprise, collaboration with internal and external stakeholders will become even more pivotal. Collaboration will facilitate greater alignment of business goals and objectives. Companies embracing security convergence and facilitating its implementation will emerge as leaders not only in their sectors but also across all sectors. The study provides strong support for the idea that managing risk effectively in a complex, dynamic environment can be achieved through convergence.

⁹ ASIS International Conference 2005, September 12–15, 2005.
<http://www.asisonline.org/education/programs/noframe/2005seminar/default.html>