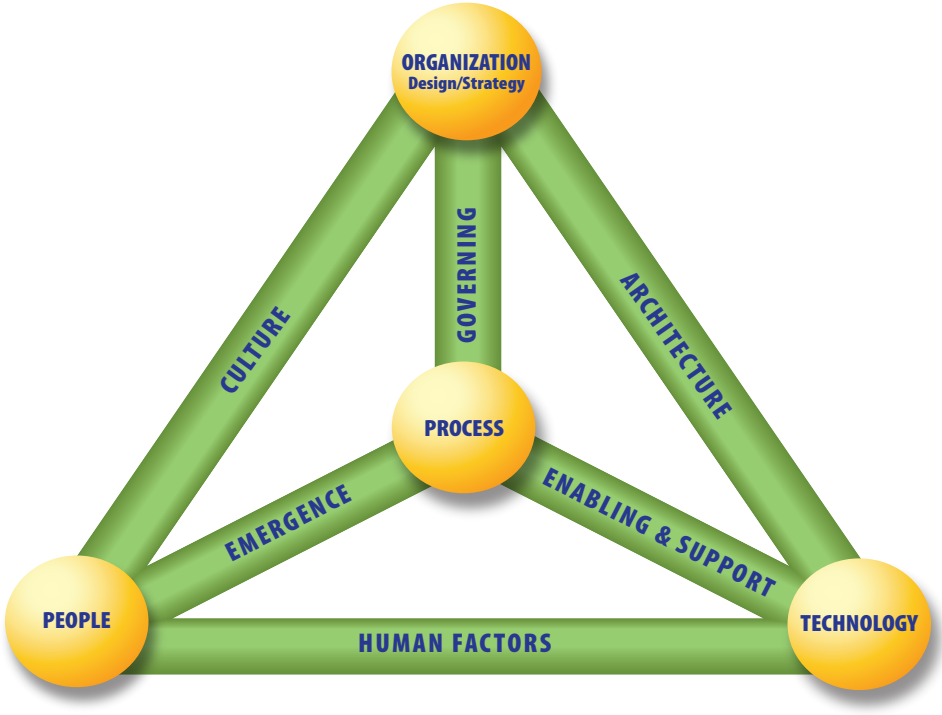
An Introduction to the **Business Model for Information Security**



ISACA®
Serving IT Governance Professionals

ISACA®
With more than 86,000 constituents in more than 160 countries, ISACA (*www.isaca.org*) is a recognized worldwide leader in IT governance, control, security and assurance. Founded in 1969, ISACA sponsors international conferences, publishes the *ISACA® Journal*, and develops international information systems auditing and control standards. It also administers the globally respected Certified Information Systems Auditor™ (CISA®) designation, earned by more than 60,000 professionals since 1978; the Certified Information Security Manager® (CISM®) designation, earned by more than 10,000 professionals since 2002; and the new Certified in the Governance of Enterprise IT™ (CGEIT™) designation.

Disclaimer
ISACA has designed and created *An Introduction to the Business Model for Information Security* (the "Work"), primarily as an informational resource for security professionals. ISACA 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, audit/assurance professionals should apply their own professional judgment to the specific circumstances presented by the particular systems or IT environment.

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

An Introduction to the Business Model for information Security
Printed in the United States of America.

Acknowledgments

ISACA wishes to recognize:

Development Team
Derek Oliver, Ph.D., CISA, CISM, Ravenswood Consultants Ltd., UK, Chair
Jean-Luc Allard, CISA, CISM, MISIS scri, Belgium
Elisabeth Antonsson, CISM, Sweden
Sanjay Bahl, CISM, India
W. Krag Brotby, CISM, Brotby and Associates, USA
Christos Dimitriadis, Ph.D., CISA, CISM, Intralot, Greece
Meenu Gupta, CISA, CISM, Mittal Technologies, USA
Cristina Ledesma, CISA, CISM, Citibank, Uruguay
Ghassan T. Youssef, CISM, Saraya Holdings, DIFC, UAE

ISACA Board of Directors
Lynn Lawton, CISA, FBCS CITP, FCA, FIIA, KPMG LLP, UK, International President
George Ataya, CISA, CISM, CGEIT, CISSP, ICT Control SA, Belgium, Vice President
Howard Nicholson, CISA, CGEIT, City of Salisbury, Australia, Vice President
Jose Angel Pena Ibarra, CGEIT, Consultoria en Comunicaciones e Info. SA & CV, Mexico, Vice President
Robert E. Stroud, CA Inc., USA, Vice President
Kenneth L. Vander Wal, CISA, CPA, Ernst & Young (retired), USA, Vice President
Frank Yam, CISA, FHKCS, FHKIoD, CCP, CFE, CFSA, CIA, FFA, Focus Strategic Group, Hong Kong, Vice President
Marios Damianides, CISA, CISM, CA, CPA, Ernst & Young, USA, Past International President
Everett C. Johnson Jr., CPA, Deloitte & Touche LLP (retired), USA, Past International President
Gregory T. Grocholski, CISA, The Dow Chemical Company, USA, Director
Tony Hayes, FCPA, Queensland Government, Australia, Director
Jo Stewart-Rattray, CISA, CISM, CSEPS, RSM Bird Cameron, Australia, Director

Security Management Committee
Jo Stewart-Rattray, CISA, CISM, CSEPS, RSM Bird Cameron, Australia, Chair
Manuel Aceves, CISA, CISM, CISSP, Cerberian Consulting, Mexico
Kent Anderson, CISM, Encurve LLC, USA
Emil D'Angelo, CISA, CISM, Bank of Tokyo-Mitsubishi UFJ Ltd, USA
Yves Le Roux, CISM, CA Inc., France
Mark Lobel, CISA, CISM, CISSP, PricewaterhouseCoopers LLP, USA
Kyeong-Hee Oh, CISA, CISM, Fullbitsoft, Korea
Vernon Richard Poole, CISM, CGEIT, Sapphire, UK
Rolf von Roessing, CISA, CISM, CGEIT, KPMG Germany, Germany

In Recognition
The Business Model for Information Security is based on research conducted by the University of Southern California's Marshall School of Business Institute for Critical Information Infrastructure Protection. ISACA wishes to recognize the contribution to the information security community that was made by Charles P. Meister, Morley Winograd, Phil Cashia, Dr. Ann Majchrzak, Dr. Ian Mitroff, Prof. Dan O'Leary, Dr. Laree Kiely, Terry Benzel, Steve Raynor and Bill Belgard, the authors of the Systemic Security Management Model.

Table of Contents

Executive Summary

In this era of global economy, ever-changing enterprise risk, cross-organization collaboration and online trade, information security has become more of a business enabler than ever thought possible. As new and evolving research, standards, tools and technologies emerge, enterprises now have the mechanisms to help secure their business transactions as well as the underlying infrastructure and information involved. Yet enterprises still struggle to keep up with regulatory requirements, economic conditions and risk management. The exact role of information security is still not clearly defined in many organizations. While some still view information security as a cost center, it has been shown that effectively managed information security organizations can be instrumental in helping an enterprise meet its business goals by improving efficiency and aligning business objectives.

Enterprises too often view information security in isolation: the perception is that security is someone else's responsibility and there is no collaborative effort to link the security program to business goals. It is easy for this compartmentalized approach to lead to weaknesses in security management, possibly resulting in serious exposure. From a financial perspective, it is possible for this lack of comprehension to result in unnecessary expenditure on security and control. From an operational perspective, information security efforts may not achieve the intended business benefit, resulting in information at risk.

Some view information security as solely a technical discipline. While IT provides tools useful in protecting information, technology alone is not the solution. To protect information, enterprises need to establish information security policies that are supported by standards, procedures and guidelines. This guidance establishes the direction for the information security program and expectations as to how information is to be used, shared, transmitted and destroyed. In many enterprises, technology strategies, policy, process and standards are developed without an understanding of how organizational culture impacts program effectiveness. Security efforts that fail to consider how humans react to and use technology often do not deliver intended benefits. Information security programs need to take into account how the organization and its people, processes and technologies interact, and how organizational governance, culture, human factors and architectures support or hinder the ability of the enterprise to protect information and to manage risk.

Information security managers have struggled to create programs that are aligned with enterprise goals and priorities, that bring value to the enterprise, and that support the ability of management to innovate while controlling risks. Developing an information security program and integrating it into business goals, objectives, strategies and activities are complicated by the lack of a model that describes what an effective information security program encompasses, how it functions, and how it relates to the enterprise and the enterprise's priorities. What is missing is a descriptive model that business unit managers and their counterparts in information security can use to talk about information security in business, rather than technical, terms.

In 2008, ISACA entered into a formal agreement with the University of Southern California (USA) Marshall School of Business Institute for Critical Information Infrastructure Protection to continue the development of its Systemic Security Management Model. The Business Model for Information Security takes a business-oriented approach to managing information security, building on the foundational concepts developed by the Institute. It utilizes systems thinking to clarify complex relationships within the enterprise, and thus to more effectively manage security.

The elements and dynamic interconnections that form the basis of the model establish the boundaries of an information security program and model how the program functions and reacts to internal and external change. The Business Model for Information Security provides the context in which frameworks such as *Control Objectives for Information and related Technology* (COBIT®)[1] and standards that enterprises currently use to structure information security program activities come together. In coming together, they form a holistic and dynamic approach to information security that is both predictive and proactive as it adapts to changes, considers the organizational culture and delivers value to the business.

[1] IT Governance Institute, COBIT® 4.1, 2008, *www.itgi.org*

1. Setting the Stage

Few would argue that enterprises have increasingly become dependent on IT to facilitate business operations. In today's knowledge-driven economy, information is critical to an enterprise's ability not only to survive, but also to thrive. Experienced business leaders know that information deserves at least the same level of protection as any other asset, and have made information security managers a common addition to the organization chart.

However, information security has struggled as a function. Security managers face myriad challenges, including changing risk profiles, lack of funding, cultural issues, and internal and external threats. Managing information security has never been so critical, yet there are very few formal models that help an information security manager do so effectively. Of the few models that do exist, even fewer consider how the enterprise changes, how the culture adapts, and what may or may not emerge as a result.

Current models tend to be static and simple, while environments are continuously changing. The Business Model for Information Security recognizes that it is a dynamic and complex world, and provides a way information security managers can take a holistic approach to managing information security while directly addressing business objectives. The model also provides a common language for information security and business management to talk about information protection.

Current Business and Security Landscape

Information security is continually evolving. Throughout history, the importance of information protection has been evident. Cryptography was an early example of a control created out of an understanding that information is a valuable asset. The relatively recent dependence on computers to facilitate business operations resulted in the development of technology-based information security solutions focused on protecting the enterprise's information infrastructures from external threats. However, as business has come to view information as a critical asset, and has increasingly come to depend on public networks to transport sensitive information, protecting information has become less about technology and more about sustainability of the enterprise itself.

The current landscape is riddled with challenges. While external issues such as rapidly changing regulatory requirements and continually shifting risks constitute primary concerns, they do not stand alone. Internal issues can prove just as thorny.

For example, although security managers and business managers are working toward the same goal, they often seem to be speaking a different language. Information security managers strive to ensure that their program helps the enterprise meet its organizational goals; this can be a difficult task, however, when they are speaking in terms of specific threats, risks, controls and technologies while business managers are talking about cost, productivity and return on investment (ROI).

The complexity of this cross-communication is compounded by the fact that security is often defined inconsistently throughout the business. For the financial manager, security may equate to minimizing financial risk and loss, while to the sales manager, it is ensuring that nothing interferes with sales efforts and achieving targets. The legal department sees it as a function of regulatory compliance, while a board member regards it as protection from personal liability. To resolve this issue, enterprises must create a culture that is supportive of information security. Everyone in the enterprise must thoroughly understand their role as it pertains to security management. The Business Model for Information Security addresses these issues by defining roles and introducing business terms—through systems thinking principles—to create a common language.

Constantly changing organizational risk profiles make enterprise security a fast-moving target. Frequently, risks are managed in silos, potentially creating additional risks to other areas in the enterprise (treating one risk can often create another, more severe). A systems thinking approach can help foster the ability to understand the interactions and consequences of addressing a particular situation, thereby avoiding a problem greater than the one being addressed. It can also help ensure that departmental isolation is reduced so the information security manager gains a better picture of information risk and how it relates to overall enterprise risk.

Due in large part to an environment of constant change, information security managers spend much of their time reacting. Working in reactive mode limits the security manager's opportunity to take the time necessary to form a holistic view: to consider the interaction of systems, possible root causes and best solutions to problems.

Instead, security "sore spots" may be treated by applying short-term fixes to symptoms, not long-term cures to the problems themselves. These fixes are often not sufficient, but they address the common expectation that implementing technology, conducting risk assessments and building processes results in security. This is not accurate, as security managers well know. For example, security weaknesses that result from inappropriate governance, inadequate management, a dysfunctional culture or unready staff cannot be fixed with technology. But, the expectation exists, and often results in enterprise leadership's disappointment with the performance of the security program.

This litany of challenges—rapidly changing risk profiles, lack of a common language, risk managed in silos and cultures that do not understand information security—is undoubtedly familiar to many enterprises. The Business Model for Information Security addresses each.

Intent of the Introduction Guide

This introduction guide, with case study, is the first document in a series planned around the Business Model for Information Security. Based on the white paper "Systemic Security Management," developed by the USC Marshall School of Business Institute for Critical Information Infrastructure Protection, this guide provides a starting point for discussion and future development. It defines the core concepts that will evolve

into practical aids information security and business unit managers can use to align security program activities with organizational goals and priorities, effectively manage risk, and increase the value of information security program activities to the enterprise. The Business Model for Information Security does not replace the many sources of security program best practices. It does, however, provide a view of information security program activities within the context of the larger enterprise, to integrate the disparate security program components into a holistic system of information protection.

This guide introduces the model and its core concepts to enterprises, particularly to:
- Senior executives
- Information security managers
- Those who have responsibility for managing business risk
- Individuals who have responsibility for the design, implementation, monitoring and improvement of an information security management system

Chapter 2 examines systems theory and the systems thinking principles that underpin the model; chapter 3 describes the model itself; chapter 4 looks at next steps; and the appendix outlines a case study in which the concepts that are fundamental to the model were used to enhance communications between a business unit and the security organization, resulting in improved information protection and business unit performance.

2. Systems Thinking

A system is an organized collection of parts (or subsystems) that are highly integrated to accomplish an overall goal. The system has various inputs, which go through certain processes to produce certain outputs, which together accomplish the overall desired goal for the system.

Systems theory is not a new concept. It dates back to the 1940s when Ludwig von Bertalanffy began to connect systems theory with wholeness. According to systems theory, a system essentially consists of objects (physical or logical), attributes that describe the objects, relationships among the objects and the environment in which the system is contained. In extension to the simple description of a system outlined in the first paragraph of this chapter, systems theory views the internal processes as more complex and, depending on the openness (or lack thereof) of the system, subject to the environment for their outputs.

The essence of systems theory is that a system needs to be viewed *holistically*—not merely as a sum of its parts—to be accurately understood. A *holistic* approach examines the system as a complete functioning unit. Another tenet of systems theory is that one part of the system enables understanding of other parts of the system.

"Systems thinking" is now a widely recognized term that refers to the examination of how systems interact, how complex systems work and why "the whole is more than the sum of its parts."[2]

Systems theory is most accurately described as a complex network of events, relationships, reactions, consequences, technologies, processes and people that interact in often unseen and unexpected ways. Studying the behaviors and results of the interactions can assist the manager to better understand the organizational system and the way it functions. While management of any discipline within the enterprise can be enhanced by approaching it from a systems thinking perspective, its implementation will certainly help with managing risk.

The success the systems approach has achieved in other fields bodes well for the benefits it can bring to security. The often dramatic failures of enterprises to adequately address security issues in recent years are due, to a significant extent, to their inability to define security and present it in a way that is comprehensible and relevant to all stakeholders. Utilizing a systems thinking approach to information security management will help information security managers address complex and dynamic environments, and will generate a beneficial effect on collaboration within the enterprise, adaptation to operational change, navigation of strategic uncertainty and tolerance of the impact of external factors.

[2] von Bertalanffy, L.; *General System Theory: Foundations, Development, Applications*, George Braziller, 1976

Although systems thinking can contribute to these beneficial outcomes, it is important to note that the Business Model for Information Security, which is based on systems theory, should be treated as part of the strategic plan for the information security program, not as a quick-fix solution for a broken program. Systems thinking should be seen as a long-term exercise that will ultimately aid the enterprise in achieving business goals. In fact, it may help to think of it as a key to organizational maturity. The maturity of the information security program is often related to the maturity of the enterprise, which is linked to the degree systemic thinking is used in the organization. Systemic thinking paves the way for systemic processes.

Business Evolution and Systems Thinking

More than ever, businesses have "gone global" as a result of expanding e-commerce capabilities among other issues. They have also increasingly begun to depend on third-party vendors for business operations (posing challenges for information security departments, which must ensure the protection of valuable customer data and internal proprietary information when communicating with other enterprises). It takes complex systems to handle these complex opportunities, and information security must keep pace.

Any security model must recognize and accommodate dynamic relationships both internal and external to the business. External relationships, such as those with third-party vendors, and internal relationships with individual business units contribute to the dynamics that shape the culture of the enterprise.

Many organizational activities relate in some manner to security, assurance or safety. Typical departments include risk management, legal, audit, compliance, privacy, business continuity, quality control, facilities, human resources, IT security, information security and physical security. Their activities tend to be viewed as silos and they are typically not connected, have different reporting structures, speak different languages and collectively may consume more than a quarter of organizational resources. Nevertheless, they are all engaged in activities that have a bearing on, or are related to, security. Integration of these activities into a model that makes explicit the interrelationships and impacts among related tasks will begin to address the issues of overall assurance process integration and more cost-effective security.

Principles of Systems Thinking

As previously stated, systems thinking is about wholeness. Looking at information security in pieces (people, process, technology) has not proven to be an effective method to manage a security program. Security-related problems are often complex and dynamic, yet all models (until now) have been simple and static. Problems have been viewed simplistically as straight-line cause and effect, when more complex (and circular) forces are generally in play. The Business Model for Information Security avoids this pitfall by employing systems thinking principles such as circular thinking, innovation, feedback and delay to help create synergy in an enterprise.

Changing business, threats, and regulatory and technological environments demand creativity and planning, not reactivity. Innovation is key to any enterprise seeking success: entering new markets with innovative new products, solutions or improvements to proven methods is critical to organizational evolution.

Feedback is an important element in obtaining the greatest benefit from innovation efforts. In systems thinking, feedback is a process of sharing observations, concerns and suggestions among persons or divisions of the enterprise for the purpose of improving both organizational and personal performance. Feedback enhances innovation and—specifically for security—is important to helping to portray security as a critical element of the enterprise as a whole.

Delay is one more concept of systems thinking that must be considered. Delays can be described as "interruptions between actions and consequences."[3] Feedback processes contain delays in the flow of influence, which make the consequences of actions occur gradually. Delays may present unique challenges in that they can lead to instability or breakdown if unrecognized, or they may have a positive effect if recognized and addressed.

Constant change calls on an enterprise's resilience. In the long term, innovation may ensure success, but dealing with the immediate upheavals of change requires resilience today.

The Intentional Information Security Culture

A critical piece of the model that differentiates it from many others is the importance it places on organizational culture. Creating an intentional security culture is a primary objective for the model, as applied to information security. To create this intentional culture many things need to be instituted:

- **Awareness campaigns**—Campaigns can consist of general information security awareness activities and targeted educational sessions for specific audiences. These sessions are good opportunities to begin to inform departments of their information security responsibilities. The human resources function may be responsible for initial awareness training for new employees; that training should incorporate material that demonstrates security's importance to the enterprise.
- **Cross-functional teams**—Risk councils and security steering committees are examples of different functional areas working together to improve the enterprise's overall security posture. These are not the only examples: the human resources function is heavily involved in entrance and exit policies, and business owners need to be involved with management of their data. The use of cross-functional teams encourages communication and collaboration and reduces departmental isolation and duplicated efforts—in turn, reducing costs and improving profitability.

[3] Senge, P.; *The Fifth Discipline: The Art and Practice of a Learning Organization*, Doubleday, 1990

- **Management commitment**—As noted previously, one of the unique attributes of this model is its focus on organizational culture. Culture constitutes the reasoning behind the method by which things get done. If the senior management team does not genuinely support the information security program, it can discourage any other employee's sense of obligation or responsibility to the program. Therefore, it is critical for the enterprise's senior management team—including the board of directors and all executives—to accept ownership for information security and genuinely support the program.

The intentional information security culture focuses on the enterprise's governance needs.[4] This type of culture has several important characteristics:

- **Alignment of information security and business objectives**—The model enables and supports business objectives. The information security program aligns with the enterprise from the boardroom to end users, and requires information security controls to be practical and provide real, measurable risk reduction.
- **A risk-based approach**—Frequently, information security controls are implemented with little or no assessment of the actual risks and threats to the enterprise, resulting in damaging underprotection or wasteful overprotection. Information security managers must understand the business—its objectives, operating and regulatory environment, potential threats, risk impacts, operational flexibility, and resilience. Only then can they select appropriate controls to mitigate risk effectively.
- **Balance among organization, people, process and technology**—Effective risk management requires organizational support, competent people, efficient processes and selection of appropriate technology. Each element interacts with, impacts and supports the other elements, often in complex ways, so it is crucial to achieve a balance among these elements. If any one element is deficient, information security is diminished.
- **Allowance for the convergence of security strategies**—To maximize RIO, all security functions (information security, physical security, etc.) should be aligned with and support each other. Nonaligned security functions are wasteful and hinder the identification and mitigation of cross-functional risk.

[4] Anderson, Kent; "A Business Model for Information Security," *Information Systems Control Journal*, vol. 3, 2008, p. 51-52

3. The Model

The Business Model for Information Security began life as a model for systemic security management, created by Dr. Laree Kiely and Terry Benzel at the USC Marshall School of Business Institute for Critical Information Infrastructure Protection. In 2008 ISACA acquired from the university the rights to develop the model to help embed its concepts in information security practices globally.

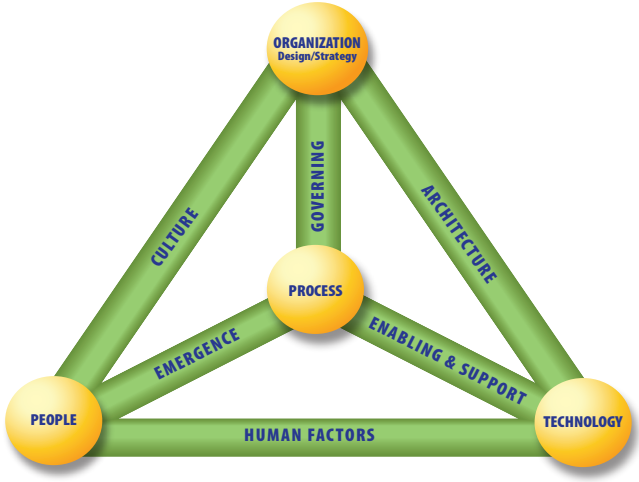
The model takes a business-oriented approach to managing information security. Its holistic and dynamic approach to information security within the context of business demonstrates to the enterprise that information security can be both predictive and proactive.

The model can be used regardless of the size of the enterprise or the information security framework (if any) the enterprise currently has in place. The model is independent of any particular technology or technological changes over time. Likewise, it is applicable across industries, geographies, and regulatory and legal systems. It includes not only traditional information security but also privacy, linkages to risk, physical security and compliance.

Structure of the Model

As illustrated in **figure 1**, the model is best viewed as a flexible, three-dimensional, pyramid-shaped structure made up of four elements linked together by six dynamic interconnections. All aspects of the model interact with each other. If any one part of the model is changed, not addressed or managed inappropriately, the equilibrium of the model is potentially at risk. The dynamic interconnections act as tensions, exerting a push/pull force in reaction to changes in the enterprise, allowing the model to adapt as needed.

Figure 1—The Business Model for Information Security



Source: Adapted from the USC Marshall School of Business Institute for Critical Information Infrastructure Protection

The Elements

The four elements of the model are:

1. **Organization Design and Strategy**—An organization is a network of people, assets and processes interacting with each other in defined roles and working toward a common goal.

   An enterprise's strategy specifies its business goals and the objectives to be achieved as well as the values and missions to be pursued. It is the enterprise's formula for success and sets its basic direction. The strategy should adapt to external and internal factors. Resources are the primary material to design the strategy and can be of different types (people, equipment, know-how).

   Design defines how the organization implements its strategy. Processes, culture and architecture are important to determining the design.
2. **People**—The people element represents the human resources and the security issues that surround them. It defines who implements (through design) each part of the strategy. It represents a human collective and must take into account values, behaviors and biases.

   Internally, it is critical for the information security manager to work with the human resources and legal departments to address issues such as:
   - Recruitment strategies (access, background checks, interviews, roles and responsibilities)
   - Employment issues (location of office, access to tools and data, training and awareness, movement within the enterprise)
   - Termination (reasons for leaving, timing of exit, roles and responsibilities, access to systems, access to other employees)

   Externally, customers, suppliers, media, stakeholders and others can have a strong influence on the enterprise and need to be considered within the security posture.
3. **Process**—Process includes formal and informal mechanisms (large and small, simple and complex) to get things done and provides a vital link to all of the dynamic interconnections. Processes identify, measure, manage and control risk, availability, integrity and confidentiality, and they also ensure accountability. They derive from the strategy and implement the operational part of the organization element.

   To be advantageous to the enterprise, processes must:
   - Meet business requirements and align with policy
   - Consider emergence and be adaptable to changing requirements
   - Be well documented and communicated to appropriate human resources
   - Be reviewed periodically, once they are in place, to ensure efficiency and effectiveness
4. **Technology**—The technology element is composed of all of the tools, applications and infrastructure that make processes more efficient. As an evolving element that experiences frequent changes, it has its own dynamic risks. Given the typical enterprise's dependence on technology, technology constitutes a core part of the enterprise's infrastructure and a critical component in accomplishing its mission.

As noted in chapter 1, technology is often seen by the enterprise's management team as a way to resolve security threats and risks. While technical controls are helpful in mitigating some types of risks, technology should not be viewed as an information security solution.

Technology is greatly impacted by users and by organizational culture. Some individuals still mistrust technology, some have not learned to use it and others feel it slows them down. Regardless of the reason, information security managers must be aware that many people will try to sidestep technical controls.

Dynamic Interconnections

The dynamic interconnections are what link the elements together and exert a multidirectional force that pushes and pulls as things change. Actions and behaviors that occur in the dynamic interconnections can force the model out of balance or bring it back to equilibrium. The six dynamic interconnections are:

1. **Governing**—Governing is the steering of the enterprise and demands strategic leadership. Governing sets limits within which an enterprise operates and is implemented within processes to monitor performance, describe activities and achieve compliance while also providing adaptability to emergent conditions.

   Governing incorporates ensuring that objectives are determined and defined, ascertaining that risks are managed appropriately, and verifying that the enterprise's resources are used responsibly.
2. **Culture**—Culture is a pattern of behaviors, beliefs, assumptions, attitudes and ways of doing things. It is emergent and learned, and it creates a sense of comfort.[5] Culture evolves as a type of shared history as a group goes through a set of common experiences. Those similar experiences cause certain responses, which become a set of expected and shared behaviors. These behaviors become unwritten rules, which become norms that are shared by all people who have that common history. It is important to understand the culture of the enterprise because it profoundly influences what information is considered, how it is interpreted and what will be done with it.

   Culture may exist on many levels, such as national (legislation/regulation, political and traditional), organizational (policies, hierarchical style and expectations) and social (family, etiquette). It is created from both external and internal factors, and is influenced by and influences organizational patterns.
3. **Enabling and support**—The enabling and support dynamic interconnection connects the technology element to the process element. One way to help ensure that people comply with technical security measures, policies and procedures is to make processes usable and easy. Transparency can help generate acceptance for security controls by assuring users that security will not inhibit their ability to work effectively.

[5] Kiely, L.; T.V. Benzel; "Systemic security management," *Security & Privacy, IEEE* 4 (6), 2006, p. 74-77

Many of the actions that affect both technology and processes occur in the enabling and support dynamic interconnection. Policies, standards and guidelines must be designed to support the needs of the business by reducing or eliminating conflicts of interest, remaining flexible to support changing business objectives, and being acceptable and easy for people to follow.

4. **Emergence**—Emergence—which connotes surfacing, developing, growing and evolving—refers to patterns that arise in the life of the enterprise that appear to have no obvious cause and whose outcomes seem impossible to predict and control. The emergence dynamic interconnection (between people and processes) is a place to introduce possible solutions such as feedback loops; alignment with process improvement; and consideration of emergent issues in system design life cycle, change control, and risk management.
5. **Human factors**—The human factors dynamic interconnection represents the interaction and gap between technology and people and, as such, is critical to an information security program. If people do not understand how to use the technology, do not embrace the technology or will not follow pertinent policies, serious security problems can evolve. Internal threats such as data leakage, data theft and misuse of data can occur within this dynamic interconnection.

   Human factors may arise because of age, experience level and/or cultural experiences. Because human factors are critical components in maintaining balance within the model, it is important to train all of the enterprise's human resources on pertinent skills.
6. **Architecture**—A security architecture is a comprehensive and formal encapsulation of the people, processes, policies and technology that comprise an enterprise's security practices. A robust business information architecture is essential to understanding the need for security and designing the security architecture.

   It is within the architecture dynamic interconnection that the enterprise can ensure defense in depth. The design describes how the security controls are positioned and how they relate to the overall IT architecture. An enterprise security architecture facilitates security capabilities across lines of businesses in a consistent and a cost-effective manner and enables enterprises to be proactive with their security investment decisions.

Using the Model

Given the pace of business today, enterprises need to understand the issues at any given time and be able to design solutions quickly and effectively. By applying systems thinking concepts, the model allows for a life-cycle approach to information security management throughout the enterprise. The model focuses on security, but once it is fully embraced, it can positively impact other functional processes as well.

The model will benefit a range of stakeholders by reducing costs, improving performance, fostering a better understanding of organizational risks, increasing collaboration and reducing duplication of effort. Diligent utilization of the model will equip enterprises to deal with current and future issues such as:

- Regulatory requirements
- Globalization
- Growth and scalability
- Organizational synergies
- Evolving technology
- Economic markets
- Human resources
- Competition
- Ever-changing threats
- Innovation

Virtually all enterprises have areas the model can help to manage more efficiently. Methods espoused in the model—such as creating a culture that intentionally accepts information security, providing awareness and training so employees understand thoroughly what information security is and how it relates to them, and considering social and psychological issues—will help improve any enterprise's security management.

Use of the model will help managers learn to address the aggregation of risks generated by the combination and interrelation of events and dynamic dimensions, rather than by cause-and-effect patterns. As a result, they can utilize the model to create tools that help people define systemic processes to better manage risk within the enterprise.

Some background work needs to be done before use of the model begins, to ensure that it has every opportunity to produce full benefits. From an organizational strategy and design perspective, it is critical for the security manager to acquire the senior management team's buy-in into the program. This will help with both cultural issues and process. Instilling proper governance perspectives will help ensure alignment of the security program with the enterprise's goals. This can lead to balance, by enabling a view of security from a business perspective and a view of business from a security perspective. It will also reiterate the importance of business managers understanding security as an organizational initiative instead of a technology initiative.

4. What's Next

This introduction to the Business Model for Information Security captures the core elements of the Systemic Security Management Model developed by the USC Marshall School of Business Institute for Critical Information Infrastructure Protection. No new research or development of ideas is included in this document. ISACA's intent is for this introductory document to serve as a starting point for development of research reports, publications and seminars—activities being led by the members ISACA's Security Management Committee, which develops and manages the security program strategy supporting ISACA members. The committee members are being aided by an international committee of information security subject experts, who are responsible for the evolution of the model and for the production of materials related to it.

The Business Model for Information Security presents a systemic view of how an information security program operates. It captures the dynamic interconnections—the forces that exert the greatest influence on information security programs and, to a great extent, determine the ability of programs to achieve their goals. The model can be used to predict how a change in technology, process, organization or human resources is impacted by culture, human factors or the other dynamic interconnections.

Many organizations already rely on standards and frameworks to define how information security is implemented within the enterprise. Many use CobiT as a guide for implementing an internal control system to link IT with business goals and for measuring success against performance metrics and maturity models. Enterprises often use standards provided by the International Organization for Standardization (ISO), and other bodies supporting specific information security requirements, to further define CobiT's processes for information security program management and information protection. The Business Model for Information Security integrates frameworks and standards for information security, defining the boundaries of an information security program and how the program functions. Existing frameworks and standards do not adequately address organizational culture or human factors, or provide for the unexpected (as the model does through the concept of emergence). Areas that are essential for the success of an information security program but that are not currently defined in frameworks and standards will be developed as part of the evolution of the Business Model for Information Security. To carry out this development, ISACA will reach out to academics, subject matter experts and practitioners on a global basis. The resulting model will provide practical aid to members of the global information security community to help in integrating information security program activities and business strategies.

An in-depth explanation of the Business Model for Information Security, examining the model and systems thinking in relation to information security programs, will be released in 2009. Additional research reports will be developed exploring the dynamic interconnections and their impact on information security program performance. Work is also expected to begin on a report that addresses systems thinking, the model and information risk as components of enterprise risk management.

Appendix—Case Study

Abstract

One of the greatest challenges in information security is aligning the goals of the security staff with the business objectives and corporate goals of the enterprise. Often, the tasks of the security team are spent on reactive and tactical activities such as remediation of operational vulnerabilities rather than enhancing the corporate strategy. This disconnect between information security operations and strategic business objectives results in pressure to control security spending while risks, incidents and losses continue escalating to unsustainable levels. However, when aligned with the business objectives of an enterprise, information security can provide an intentional and powerful ally and source for competitive advantage, creating support for additional expenditures for this function.

Background

In early 2005, the sales division of a *Fortune* 50 company was experiencing significantly declining sales. While the sales division believed it was due to increased market competition and pricing pressures from their customers, the security group believed that lack of proper security procedures was contributing to the decline. As specific factors in the decline, they named the loss of proprietary data by traveling sales personnel, vulnerable network security systems and procedures, and a refusal by the sales force to adhere to corporate security guidelines and policies. There was a fundamental lack of alignment between the security function and the line sales force with regard to people, processes, organization and technology, and it was inhibiting the ability of the company to meet its sales and corporate goals.

During this time, the company decided to enhance the role of the chief security officer (CSO) to accommodate the changing demands of its customers and the global security challenges facing the enterprise. Around the same time, the global head of sales was replaced and a new executive with a broader perspective of the company's challenges was promoted from within to take over the sales function. The CSO knew that there were significant issues within the sales group but had not been able to initiate any change due to its past leadership and culture. As part of the process for improving the security of critical sales and marketing information within the corporation, the new head of sales and the CSO jointly agreed to sponsor the implementation of the Business Model for Information Security.

The challenge would be to effectively instill an intentional security culture within a sales organization that did not view security as necessary to their jobs.

Process

It was imperative that all executives from both groups understood the value of aligning security with the business objectives of the enterprise. After the leaders of the sales and security organizations agreed on the value to their departments of such alignment, they established a strategy council consisting of members from the security, sales and

marketing teams. The strategy council was charged with drafting a description of the future state and a statement of principles.

Interviews with members of the sales and security groups were conducted over several weeks. The information collected from these interviews was used to create a document that described how security could look and operate across the sales group in the future. The intent of the document was to create a common vision of how to achieve the goals of maintaining secure business information while ensuring a flexible and dynamic sales process.

The statement of principles outlined the critical security principles for guiding decision making and helping set security priorities in the future. The council established how to define security-related technology that should be utilized by the business to better protect critical information and maintain a safe and secure workplace. It also described security processes/protocol that would increase the security of critical information while supporting business processes. The council outlined what a high level of commitment to the security process among employees would look like and how it would be achieved. Finally, the council identified how enterprise leadership would create an intentional security culture that recognizes security as a competitive advantage. In short, the goal was to create a mind shift within the sales organization with regard to technology, process, people and organization—a shift from a functional security culture to an intentional security culture (**figure 2**).

Figure 2—Shifting From Functional to Intentional Security Culture

From	To
Move Technology	
• Unsure about the level of security the technology provides • Seeing security-related technology as disruptive and cumbersome to use	• Technology used is based on an assessment of the risk. • Seeing new security technology as a means to enhance the sales process
Move Process	
• Security brought in when there is a suspected breach • Security maintains expert knowledge.	• Security involvement in the earliest planning phases of campaigns • Security shares its knowledge and expertise, developing broader security awareness across the enterprise.
Move People	
• Security as an entity that enforces compliance • Security as a functional expert	• Security as a partner that creates awareness and commitment • Security as a partner that transfers security knowledge and expertise to its sales customers
Move Enterprise	
• Limited visibility or awareness of security issues • Security structure focused on technical expertise	• Receiving regular updates about potential risk • Security structure supports processes of its customers.

The workshops that were used to help create this cultural shift dealt with:
- Improving the partnership between security and sales
  - Creating an annual "state of risk" address
  - Designing a security structure that would support the sales process
- Defining and coordinating sales campaigns and key events for coming year
  - Highest-risk campaigns and events jointly defined
- Conducting a risk assessment
  - Intelligence sources included information from:
    - In-country employees
    - Nonintelligence forces
  - Security plan for sales campaign
    - Appropriate people, processes and technology defined for each
  - Focused on keeping information secure, using appropriate technology, heightening awareness, ensuring processes and protecting personnel
- Security support of sales campaign
  - Security orientation training available for sales campaign members
  - Executing security strategy
  - Partnering to address security issues identified during campaign
  - Transfer of security knowledge and campaign to sales
- Post-campaign assessment
  - Security effectiveness assessed
  - Lessons learned from the campaign shared with security and sales

Conclusion

There were many outcomes of the model's implementation that created an alignment of security's and the sales organization's goals for the enterprise. One finding of the workshops was that many in the sales organization were not sure which mechanism was the best to use to keep information secure. Today, sales personnel can use the intranet to access a recommended protocol based on the region and country where business is being conducted. Further, within each sales campaign where security is partnering with sales, the risk assessment will help identify the technology protocol appropriate for the specific campaign.

Security's familiarity with the sales process has enhanced its ability to identify the latest technologies that might be useful to sales personnel out in the field. On a regular basis, security assesses new technology and makes specific recommendations to the sales directors about security enhancements during sales campaigns. In 2006, recommendations from the security organization helped improve the level of security during conference calls. Similarly, in partnership with the sales organization, the security group tested the security of international cell phones.

Being able to enjoy the convenience of a cell phone while not worrying about being monitored by outsiders was identified as a means to enhance the sales process. In working with vendors and assessing new controls, the security organization keeps in mind the transparency principle: the new control must be no more difficult to use than the one it is replacing. For example, making and answering phone calls from

an encrypted international cell phone must not be more difficult than calling from a standard cell phone. The reason: more secure methods simply will not be used if they prove to be more cumbersome than commonly used methods already in place. To the greatest extent possible, the enhanced security features must be transparent to the user.

Through its risk assessments, security also helps its customers make decisions on the speed and expense of adopting new security mechanisms. In 2006, there were instances of security advising for and against purchasing new technology based on the level of threat, vulnerability and potential impact identified by the risk assessment. The sales organization now seeks assistance from security as soon as a sales campaign opportunity has been defined.

There is widespread recognition that coming to security after there has been a suspected security breach is too late; planning and preparation are critical. Today, sales and security work together in the earliest stages of sales campaigns to assess risk and jointly define appropriate actions.

As a means to transfer learning across the security organization and to its customers, a formal process for reviewing security effectiveness on selected campaigns was initiated. These security assessments were patterned after the reviews sometimes completed by the sales teams at the end of their campaigns. Whenever a customer identifies a successful example of security effectiveness, the security personnel involved are asked to present the example and explain what was learned. This has helped to create more awareness of security successes in addition to learning from security breaches.

These examples of successful and not-so-successful security activities are considered for more detailed case study analysis. These case studies include background information, the nature of the success or breach, an analysis of what was learned, and recommendations for the future. Case studies are shared across the security organization and with appropriate customers.

By 2007, the risk assessment model introduced by security had become part of the vocabulary of sales directors and managers. During a campaign, sales directors will often refer to the risk assessment model and ask questions about the nature of a threat, the extent to which the enterprise is vulnerable or the degree of likely impact. The widespread use of this language indicates how ingrained the risk assessment model has become. The reason for this acceptance is the consistency with which the risk assessment process is used by security personnel and their ability to engage their customers in assessing risk and providing meaningful recommendations.

Regional security managers make it a priority to connect regularly with the sales director working on campaigns in their territory to learn about the inner workings of the campaign and the potential security issues that could emerge during its course. Today, each regional sales director has a direct contact point with the security organization. This contact is located where the majority of the sales team he/she supports resides, enabling

easy, direct, face-to-face contact. The contact is someone the sales director knows, who regularly attends and contributes to the sales staff meetings, and who has added value to critical sales campaigns by helping assess risk and jointly develop security plans.

For the sales directors, their security contact is a member of the sales team and an important contributor to the planning and execution of key sales campaigns. Sales managers report that the security expertise brought to their team during campaigns has given them more confidence that the competition is "not capturing our information and using it against us."

Security believes that an important part of its role today is to transfer knowledge to its clients in the sales organization about how to maintain secure information and protect team members operating in foreign countries. While this practice of "training the trainer" is fairly new, it has already begun to pay significant dividends in heightening the sales personnel's awareness of security-related issues.

In regions where a strong relationship exists between sales personnel and security, there has been a solid transfer of basic knowledge and awareness. In these areas, employees have been educated on and held accountable to a heightened awareness of how information is leaked and the appropriate protocol to follow to prevent it. Already there is considerable anecdotal information to suggest that the teams in which these practices are in place have fewer security incidents. Some of the specific practices include:

- Conducting a risk assessment and determining where expertise from the security organization is of the most value
- Finding and utilizing information posted by the security organization on the company intranet site
- Using security orientations for members new to the country and/or sales campaign (These orientation sessions were originally developed by security, with input from sales. The information in the orientation sessions is customized to be relevant to the country where the campaign is occurring.)
- Being aware of travel information containing the perspectives of in-country field representatives
- Using a technology kit, which consists of the appropriate technologies to be used during the campaign, such as encrypted handheld devices, appropriate user manuals, and disposable cell phones

Starting in 2006, the security organization began tracking security incidents and reported suspicious activities. Security reviews the information, looks for patterns and regularly shares the findings with sales. An unanticipated outcome of this information sharing has been the creation of a heightened sense of awareness. Today, many incidents are disclosed that were unreported in the past or were seen as stolen property issues rather than as possible losses of corporate sensitive information.

Having a clearer picture of security incidents has helped security and sales better define ways to prevent future occurrences. Security awareness across the sales organization

has been heightened and greater information sharing can be seen at all levels, starting with the yearly security briefing the CSO gives to the sales organization during its annual meeting. In this briefing, sometimes referred to as the "state of risk" address, the CSO describes instances where information, property or personal safety has been compromised during the previous year and explains what can be learned from the incidents. The presentation also describes emerging risks, based on security intelligence, and offers high-level recommendations to mitigate those risks. The information gained from the briefing is summarized, packaged and made available to members of the sales executive team to roll out to the entire sales organization.

In 2006, the company experienced record sales, reversing several years of decline, and its stock price soared by more than 25 percent.

Other Publications

Many publications issued by the IT Governance Institute® (ITGI™) and ISACA contain detailed assessment questionnaires and work programs. For further information, please visit *www.isaca.org/bookstore* or e-mail *bookstore@isaca.org*.

Security

- *Cybercrime: Incident Response and Digital Forensics*, 2005
- *Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition*, 2006
- *Information Security Governance: Guidance for Information Security Managers*, 2008
- *Information Security Harmonisation—Classification of Global Guidance*, 2005
- *Managing Enterprise Information Integrity: Security, Control and Audit Issues*, 2004
- *Security Awareness: Best Practices to Serve Your Enterprise*, 2005
- *Stepping Through the InfoSec Program*, 2007

Assurance

- *ITAF™: A Professional Practices Framework for IT Assurance*, 2008
- *Stepping Through the IS Audit, 2nd Edition*, 2004

ERP Series:

- *Security, Audit and Control Features Oracle® E-Business Suite: A Technical and Risk Management Reference Guide, 2nd Edition*, 2006
- *Security, Audit and Control Features PeopleSoft®: A Technical and Risk Management Reference Guide, 2nd Edition*, 2006
- *Security, Audit and Control Features SAP®R/3®: A Technical and Risk Management Reference Guide, 2nd Edition*, 2005

Specific Environments:

- *Electronic and Digital Signatures: A Global Status Report*, 2002
- *Enterprise Identity Management: Managing Secure and Controllable Access in the Extended Enterprise Environment*, 2004
- *Linux: Security, Audit and Control Features*, 2005
- *Managing Risk in the Wireless LAN Environment: Security, Audit and Control Issues*, 2005
- *Oracle® Database Security, Audit and Control Features*, 2004
- *OS/390—z/OS: Security, Control and Audit Features*, 2003
- *Risks of Customer Relationship Management: A Security, Control and Audit Approach*, 2003
- *Security Provisioning: Managing Access in Extended Enterprises*, 2002
- *Virtual Private Network—New Issues for Network Security*, 2001

IT Governance

- *Board Briefing on IT Governance, 2nd Edition*, 2003
- *Identifying and Aligning Business Goals and IT Goals*, 2008
- *IT Governance Global Status Report—2008*
- *Understanding How Business Goals Drive IT Goals*, 2008

COBIT and Related Publications

- COBIT® 4.1, 2007
- *COBIT® Control Practices: Guidance to Achieve Control Objectives for Successful IT Governance, 2nd Edition*, 2007
- *COBIT® Quickstart™, 2nd Edition*, 2007
- *COBIT® Security Baseline™, 2nd Edition*, 2007
- *IT Assurance Guide: Using COBIT®*, 2007
- *IT Control Objectives for Basel II: The Importance of Governance and Risk Management for Compliance*, 2007
- *IT Control Objectives for Sarbanes-Oxley: The Role of IT in the Design and Implementation of Internal Control Over Financial Reporting, 2nd Edition*, 2006
- *IT Governance Implementation Guide: Using COBIT® and Val IT™, 2nd Edition*, 2007
- *IT Governance and Process Maturity*, 2008
- *Unlocking Value: An Executive Primer on the Critical Role of IT Governance*, 2008

COBIT Mapping Series:

- *Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit*, 2008
- *COBIT® Mapping: Mapping of CMMI® for Development V1.2 With COBIT® 4.0*, 2007
- *COBIT® Mapping: Mapping of ISO/IEC 17799:2000 With COBIT® 4.0, 2nd Edition*, 2006
- *COBIT® Mapping: Mapping of ISO/IEC 17799:2005 With COBIT® 4.0*, 2006
- *COBIT® Mapping: Mapping of ITIL V3 With COBIT® 4.1*, 2008
- *COBIT® Mapping: Mapping of NIST SP800-53 With COBIT® 4.1*, 2007
- *COBIT® Mapping: Mapping of PMBOK With COBIT® 4.0*, 2006
- *COBIT® Mapping: Mapping of PRINCE2 With COBIT® 4.0*, 2007
- *COBIT® Mapping: Mapping of SEI's CMM for Software With COBIT® 4.0*, 2006
- *COBIT® Mapping: Mapping of TOGAF 8.1 With COBIT® 4.0*, 2007
- *COBIT® Mapping: Overview of International IT Guidance, 2nd Edition*, 2006

IT Governance Domain Practices and Competencies:

- *Governance of Outsourcing*, 2005
- *Information Risks: Whose Business Are They?*, 2005
- *IT Alignment: Who Is in Charge?*, 2005
- *Measuring and Demonstrating the Value of IT*, 2005
- *Optimising Value Creation From IT Investments*, 2005

Val IT:

- *Enterprise Value: Governance of IT Investments, Getting Started With Value Management*, 2008
- *Enterprise Value: Governance of IT Investments, The Business Case*, 2006
- *Enterprise Value: Governance of IT Investments, The Val IT Framework 2.0*, 2008
- *Enterprise Value: Governance of IT Investments, The Val IT Framework 2.0 Extract*, 2008

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