

# A Business Model for Information Security

By Kent Anderson, CISM

One of the greatest challenges in information security is aligning with business objectives. While practitioners talk about incorporating governance and business requirements, the reality tells a different story. A recent survey showed that 50 percent of North American security professionals' time is spent on reactive and tactical activities such as remediation of operational vulnerabilities.<sup>1</sup> This disconnect between information security operations and strategic business objectives results in pressure to increase security spending while risks, incidents and losses continue escalating to unsustainable levels.

A framework enabling information security professionals to align their activities with their organization's business is needed.

## The Current State of Information Security

Security awareness is at an all-time high. Organizations are spending and hiring information security practitioners in record numbers, and legislation and regulations are proliferating. Despite all of this effort, nearly every statistical measure of performance—from the number of incidents and vulnerabilities to the cost and impact of a breach—demonstrates that the problems are getting worse. More money and technology will not reverse this trend. In what other profession would this level of investment be permitted with such poor return?

The information security profession suffers from several problems that lead to a disconnect between the business and the information security program. Arguably, the greatest is the myopic focus on technology. Many practitioners in the information security field are information technology (IT) engineers and technicians who just “fall into security.” Their training and background is technical, so they overlook the elements that technology depends on: organization, people and process. Effective information security requires a balance among these elements.

This technical focus can isolate the information security function from the other stakeholders in an organization and can create a gap between information security and the business units. Organizational leaders are concerned with other risks, such as physical security, legal, financial and safety, in addition to information and technology. Too often, both sides fail to understand how all of these risks are interrelated.

Effective governance requires organizations to:

- Identify relevant risks
- Determine if security investments are appropriate
- Apply effective and efficient controls
- Align security practices to support and enable the business

Executives and boards of directors are demanding a greater return on their information security investments, and

unbalanced security programs cannot deliver the required value.<sup>2</sup> Information security projects frequently fail to meet the business objectives of the organization.

## The Solution: A Business Model for Security

Today's security functions are too often *ad hoc*, reactive and tactically focused.<sup>3</sup> What is needed is a new information security model focused on business, not technology—one that blends technology with the strategic direction and needs of the organization. This can be accomplished by creating an “intentional information security culture” focused on the organization's governance needs. An intentional security culture has several important characteristics:

- **Aligned information security and business objectives**—The model must enable and support business objectives. The information security program should align with the organization from the boardroom to end users, and information security controls should be practical and provide real, measurable risk reduction.
- **A risk-based approach**—Information security controls often are implemented with little or no assessment of the actual risks and threats to an organization, which results in failure to protect valuable assets or wasteful overprotection. Information security practitioners must understand the business—its objectives, operating and regulatory environment, potential threats, risk impacts, operational flexibility, and resilience. Only then can appropriate controls be selected to mitigate risk effectively.
- **Balance between organization, people, process and technology**—Effective risk management requires organizational support, competent people, efficient processes and the 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 return on investment, all security functions (information security, physical security, etc.) should be aligned and support each other. Nonaligned security functions are wasteful and hinder the identification and mitigation of cross-functional risk.
- **Technical and environment neutrality**—The model needs to be independent of any particular technology or technical changes over time. Likewise, the information security model should be applicable across industries, geographies, and regulatory and legal systems.

## The Model's Origin: MSB's Systemic Security Management Framework

The University of Southern California (USC)'s Marshall School of Business (MSB) formed the Institute for Critical Information Infrastructure Protection (ICIIP) to investigate ways to protect information infrastructures. The ICIIP's research led to the development of the Systemic Security Management framework.<sup>4</sup> This framework takes the traditional elements of people, processes and technology, and adds organizational design and strategy. The Systemic Security Management model recognizes that these elements (referred to as nodes) are interrelated and connected in dynamic and sometimes conflicting or competing ways. The interactions between nodes are called tensions. The critical security elements and their tensions are shown in figure 1.

Figure 1—MBS Systemic Security Management Framework



Source: Kiely, L.; T. Benzel; "Systemic Security Management: A New Conceptual Framework for Understanding the Issues, Inviting Dialogue and Debate, and Identifying Future Research Needs," Institute for Critical Information Infrastructure Protection (ICIIP), University of Southern California Marshall School of Business, USA, 23 April 2006

The addition of organization as a key element on the systemic model addresses a significant issue with many information security programs: the disconnect from the other stakeholders in the organization.

As defined by the USC paper, "organization" encompasses the "structures and strategies that enable the enterprise to compete effectively, create competitive advantages, understand its tolerance to risk and adapt governance policies that elevate security to a first priority, a board level issue, pervasive throughout the enterprise."<sup>5</sup>

From an information security practitioner's perspective, the interplay and dependencies among these elements—the tensions—create the opportunity to align the information security program with the business by focusing on the issues that too often are overlooked. The tensions are culture, governance, architecture, human factors, enabling and support, and emergence. Emergence "is a dynamic process of patterns occurring over time that seem not to be created by a single entity, person, event or rule..."<sup>6</sup> and represents the complex interactions between people and the processes (both formal and informal) used to perform their job.

These tensions interact with each other and the nodes in complex, dynamic and sometimes competing ways. The role of information security is not to eliminate these tensions, but rather to recognize and understand their effect of risk. Recognizing these tensions creates a more comprehensive information security program by addressing the whole organization. For example, some of the benefits gained when the tensions are considered include:

- Incorporating the needs of different stakeholders
- Recognizing new and unidentified risks and evaluating them cross-functionally
- Linking different information security value chains within the context of the extended enterprise (i.e., manage the loss of perimeter)
- Facilitating the analysis of risks and control implementations on the whole organization

A critical component of this new model is that the technology element is not restricted to a particular vendor, architecture, protocol or standard and, more important, focus is not on the technology, but rather the interaction of the technology with the rest of the organization; therefore, it is technology neutral.

## Next Steps

ISACA's Security Management Committee (SMC) recognizes the need to unify information security with the business mission of the organization. To this end, the SMC is currently investigating MSB's Systemic Security Management framework as the basis for a new business model for information security. A critical requirement is to turn the theoretical framework into a working model that can be used by information security practitioners. This requires the careful definition of terms, a better understanding of the tensions and the development of assessment capabilities.

The SMC also recognizes the need for the resulting model to:

- Address the business needs of organizations
- Apply internationally across different cultures and regulatory environments
- Scale from small to large organizations
- Be suitable to all types of organizations—profits, nonprofits, governmental bodies, etc.

ISACA believes the Systemic Security Management model can be developed to meet all of these requirements, allowing information security professionals to align with their organization's business objectives.

## Endnotes

- <sup>1</sup> Deloitte & Touche LLP and Ponemon Institute, "Enterprise@Risk: Insights into the Emerging Privacy and Data Protection Function," 2007
- <sup>2</sup> Anderson, K.E.; "Convergence: A Holistic Approach to Risk Management," *Network Security*, vol. 2007, iss. 5, May 2007
- <sup>3</sup> *Op cit*, Deloitte & Touche
- <sup>4</sup> Kiely, L.; T. Benzel; "Systemic Security Management: A New Conceptual Framework for Understanding the Issues, Inviting Dialogue and Debate, and Identifying Future Research Needs," Institute for Critical Information

Infrastructure Protection (ICIIP), University of Southern  
California Marshall School of Business, USA, 23 April 2006

<sup>5</sup> *Ibid.*

<sup>6</sup> *Ibid.*

### **Author's Note:**

The author would like to thank the members of ISACA's Security Management Committee for their assistance and support in the development of this article.

### ***Kent Anderson, CISM***

is a leading authority on security, with more than 22 years of experience in the field. He serves on ISACA's Security Management Committee and is the founder and managing director of Network Risk Management LLC.

*Information Systems Control Journal* is published by ISACA. Membership in the association, a voluntary organization serving IT governance professionals, entitles one to receive an annual subscription to the *Information Systems Control Journal*.

Opinions expressed in the *Information Systems Control Journal* represent the views of the authors and advertisers. They may differ from policies and official statements of ISACA and/or the IT Governance Institute® and their committees, and from opinions endorsed by authors' employers, or the editors of this *Journal*. *Information Systems Control Journal* does not attest to the originality of authors' content.

© 2008 ISACA. All rights reserved.

Instructors are permitted to photocopy isolated articles for noncommercial classroom use without fee. For other copying, reprint or republication, permission must be obtained in writing from the association. Where necessary, permission is granted by the copyright owners for those registered with the Copyright Clearance Center (CCC), 27 Congress St., Salem, Mass. 01970, to photocopy articles owned by ISACA, for a flat fee of US \$2.50 per article plus 25¢ per page. Send payment to the CCC stating the ISSN (1526-7407), date, volume, and first and last page number of each article. Copying for other than personal use or internal reference, or of articles or columns not owned by the association without express permission of the association or the copyright owner is expressly prohibited.

[www.isaca.org](http://www.isaca.org)