Carnegie Mellon
Software Engineering Institute

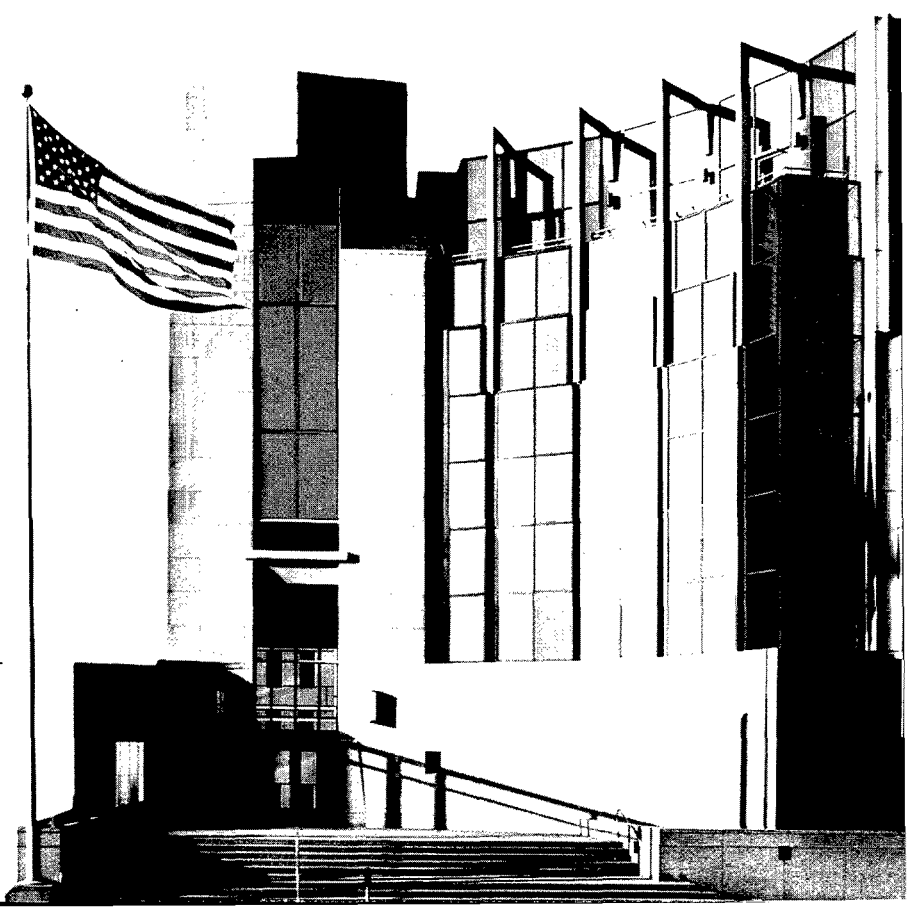
Governing for Enterprise Security

Julia Allen

June 2005

Networked Systems Survivability Program

Technical Note
CMU/SEI-2005-TN-023



Governing for Enterprise Security

Julia Allen

June 2005

Networked Systems Survivability Program

Technical Note
CMU/SEI-2005-TN-023

Contents

List of Tables

Acknowledgments

Many individuals have contributed significantly to this report by giving generously of their time, knowledge, expertise, and experience. Their contributions are expressed in the formulation of ideas, concepts, approaches, guidelines, and recommendations, and ensuring through extensive review, rewrite, and edit that these are clearly and accurately portrayed.[1] The author extends thanks and appreciation to these contributors.

External Collaborators, Interviewees, and Reviewers

- Steve Attias
  Chief Information Security Officer, New York Life Insurance Company
- Robert Charette
  President/Chief Risk Officer, ITABHI Corporation
- Larry Druffel
  President, Director & CEO, SCRA
- Amy DuVall
  Counsel & Responsible Care®[2] Advisor, American Chemistry Council
- Michael Gerdes
  Research Director, I-4 Program, Getronics RedSiren Security Solutions
- Gene Kim
  CTO, Tripwire
- Clint Kreitner
  President & CEO, The Center for Internet Security
- Alexandra Lajoux
  Chief Knowledge Officer, National Association of Corporate Directors
- Al Loeser
  Manager of Information Security, Proctor & Gamble
- Robert McMillan, formerly of CERT/CC and AusCERT
- Bev Mitchum
  Director, IT Security and Compliance, IT Services, California State University, Los Angeles
- Bryan Palma
  Chief Information Security Officer, PepsiCo, Inc.
- Heriot Prentice
  Director, Technology Practices, The Institute of Internal Auditors
- Peter Quan
  Vice President & CTO, IT Services, California State University, Los Angeles

1 The author takes full responsibility for interpretation, errors, and omissions.

2 Responsible Care is a registered service mark of the American Chemistry Council.

- Howard Schmidt, former Cyber Security Advisor, U.S. White House
  President & CEO, R&H Security Consulting LLC
- Ann Seltzer, CISSP
- George Spafford
  President, Spafford Global Consulting, Inc.
- Dan Swanson
  Director, Professional Practices, The Institute of Internal Auditors
- Jay Taylor
  General Director - IT Audit, General Motors Corporation
- Kenneth Tyminski
  Chief Information Security Officer, Prudential Financial, Inc.
- Lee Zeichner
  President, Zeichner Risk Analytics, LLC

SEI Collaborators and Reviewers

- Members of the Networked Systems Survivability Enterprise Security Management Team: Richard Caralli, Andrew Moore, James Stevens, Bradford Willke, William Wilson, Carol Woody
- Christopher Alberts
- Lisa Brownsword
- Dawn Capelli
- Audrey Dorofee
- Robert Ferguson
- Eileen Forrester
- Georgia Killcrece
- Jerry Pottmeyer
- Robin Ruefle

The author extends special thanks to Eileen Forrester and William Pollak for their guidance and assistance in creating the final version of this report; to Sheila Rosenthal, manager of the SEI Library, for her excellent research support and detective work in finding exactly the right source at exactly the right time; and to Barbara White and Laura Bentrem for their editing support.

The author greatly appreciates the ongoing support, encouragement, and guidance from the managers within the Networked Systems Survivability program who sponsored this work: Barbara Laswell, William Wilson, and Richard Pethia.

Executive Summary

In today's economic, political, and social environment, addressing security is becoming a core necessity for most, if not all, organizations. Customers are demanding it as concerns about privacy and identity theft rise. Business partners, suppliers, and vendors are requiring it from one another, particularly when providing mutual network and information access. Espionage through the use of networks to gain competitive intelligence and to extort organizations is becoming more prevalent. National and international regulations are calling for organizations (and their leaders) to demonstrate due care with respect to security.

Consider what it costs you if

- customer data is compromised and it makes the headlines
- your brand and reputation are negatively affected by a security breach, resulting in a loss of investor and consumer confidence and loyalty
- sensitive intellectual property (such as trade secrets and new product information) is stolen by a competitor or made public
- your organization is found to be non-compliant with regulations (national, state, local) as they relate to the protection of information and information security
- your network goes down because of a security breach
- you can't detect a security breach

Increasingly, an organization's ability to take advantage of new opportunities often depends on its ability to provide open, accessible, available, and secure network connectivity and services. Having a reputation for safeguarding information and the environment within which it resides enhances an organization's ability to preserve and increase market share. Opportunities deriving from an effective security program could include

- enabling new types of products and services, and new channels to new markets
- communicating with customers in a reliable, cost-effective, and timely manner
- allowing transactions to occur with greater integrity and privacy, thus ensuring business throughput, customer satisfaction, and customer confidence, which can all help create and sustain customer loyalty
- enabling profitable new types of customer/supplier engagements; interacting in a more timely and reliable way with the organization's supply chain
- providing more secure access by internal and external staff to enterprise applications

Establishing and maintaining confidence in an organization's security and privacy posture increase the likelihood that customers will refer others to the products and services offered by the organization. In addition, being viewed as an ethical organization with a culture of doing the right things and doing things right (including security) has tangible value in the international marketplace, as does being able to reliably demonstrate compliance and duty of care with respect to applicable regulations and laws.

Security As a Governance Concern

For this report, we define "governance" as setting clear expectations for the conduct (behaviors and actions) of the entity being governed, and directing, controlling, and strongly influencing the entity to achieve these expectations. It includes specifying a framework for decision making, with assigned decision rights and accountabilities, intended to consistently produce desired behaviors and actions. Governance relies on well-informed decision making and the assurance that such decisions are routinely enacted as intended. Governance is most effective when it is systemic, woven into the culture and fabric of organizational behaviors and actions. Governance actions create and sustain the connections among principles, policies, processes, products, people, and performance.

Enterprise security is important to almost all organizations. But with so many other topics vying for leadership attention, what priority should be assigned to enterprise security? What constitutes adequate security and what constitutes adequate oversight of it? How can leaders use governance to sustain adequate security in a constantly changing business, customer, risk, and technology environment?

Adequate security is about managing risk. Governance and risk management are inextricably linked—governance is an expression of responsible risk management, and effective risk management requires efficient governance. Inserting security into ongoing governance and risk management conversations is an effective and sustainable approach for addressing security.

Art Coviello, president and CEO at RSA Security and co-chair of the Corporate Governance Task Force,[3] states that "It is the fiduciary responsibility of senior management in organizations to take reasonable steps to secure their information systems. Information security is not just a technology issue, it is also a corporate governance issue" [Braun 04]. As a result, director and officer oversight of corporate digital security is embedded within the fiduciary duty of care owed to company shareholders.

In the absence of some type of meaningful governance structure and way of measuring enterprise security, the following questions naturally arise:

- How can an organization know what its greatest security risk exposures are?
- How can an organization know if it is secure enough

[3] Convened after the National Cybersecurity Summit of 2004 [CGTF 04]. See also Appendix A.

- to detect and prevent security events that require business-continuity, crisis-management, and disaster-recovery actions?
- to protect stakeholder interests and meet stakeholder expectations?
- to ensure enterprise viability?

Governing for enterprise security means viewing adequate security as a non-negotiable requirement of being in business. To achieve a sustainable capability, enterprise security must be addressed at a governance level by organizational leaders and not be relegated to a technical specialty within the IT department. The role of boards of directors, senior executives, and indeed all managers includes establishing and reinforcing the business need for effective enterprise security. Otherwise, the organization's desired state of security will not be articulated, achieved, or sustained. If the responsibility for enterprise security is relegated to a role in the organization that lacks the authority, accountability, and resources to act and enforce, enterprise security will not be optimal.

Characteristics of Effective Enterprise Security Governance[4]

Business objectives guide and drive actions needed to govern for enterprise security. The connection to business objectives is evident from a list of organizational assets that can be negatively affected if security governance is performed poorly such as trust, reputation, brand, stakeholder value, customer retention, and the ability to offer and fulfill business transactions. Organizations are much more competent in addressing this subject if their leaders are aware of and knowledgeable about the issues and treat the governance of enterprise security as essential to their business.

For the past 18 months, Carnegie Mellon University's Software Engineering Institute has conducted in-depth discussions and interviews, workshops, and work with a wide range of organizations committed to improving their security capabilities. Based on this work, they've identified the following set of beliefs, behaviors, capabilities, and actions that consistently indicate that an organization is addressing security as a governance concern:

- Security is enacted at an enterprise level. C-level[5] leaders understand their accountability and responsibility with respect to security for the organization, for their stakeholders, and for the communities they serve including the Internet community, and for the protection of critical national infrastructures.
- Security is treated the same as any other business requirement. It is considered a cost of doing business, not a discretionary or negotiable budget-line item that needs to be regularly defended. Business units and staff don't get to decide unilaterally how much security they want. Adequate and sustained funding and allocation of security resources are required as part of the operational projects and processes they support.

---

[4] Some of this material previously appeared in "How Do I Know If I Have a Culture of Security?" [Allen 05b].

[5] See Appendix C, C-Level Target Audience.

- Security is considered during normal strategic and operational planning cycles. Security has achievable, measurable objectives that directly align with enterprise objectives. Determining how much security is enough equates to how much risk and how much exposure an organization can tolerate.
- All function and business unit leaders within the organization understand how security serves as a business enabler (versus an inhibitor). They view security as part of their responsibility and understand that their performance with respect to security is measured as part of their overall performance.
- Security is integrated into enterprise functions and processes. These include risk management, human resources (hiring, firing), audit/compliance, disaster recovery, business continuity, asset management, change control, and IT operations. Security is actively considered as part of new-project initiation and ongoing project management, and during all phases of any software-development life cycle (applications and operations).
- All personnel who have access to enterprise networks understand their individual responsibilities with respect to protecting and preserving the organization's security condition. Rewards, recognition, and consequences with respect to security policy compliance are consistently applied and reinforced.

Which of these statements and actions are most important depends on an organization's culture and business context. C-level leaders committed to dealing with security as a governance-level concern can use these statements to determine the extent to which this perspective is present (or needs to be present) in their organizations.

This technical report examines governance thinking, principles, and approaches and applies them to the subject of enterprise security. Its primary intent is to increase awareness, understanding, and education of the issues, opportunities, and possible approaches for treating security as a governance concern. In addition, this report identifies resources that leaders can use both within their organizations and with their networked partners, suppliers, and customers.

Most senior executives and managers know what governance means and their responsibilities with respect to it. Our intent here is to help leaders expand their governance perspectives to include security and incorporate enterprise-wide security thinking into their own and their organizations' day-to-day governance actions.

Abstract

Governing for enterprise security means viewing adequate security as a non-negotiable requirement of being in business. If an organization's management—including boards of directors, senior executives, and all managers—does not establish and reinforce the business need for effective enterprise security, the organization's desired state of security will not be articulated, achieved, or sustained. To achieve a sustainable capability, organizations must make enterprise security the responsibility of leaders at a governance level, not of other organizational roles that lack the authority, accountability, and resources to act and enforce compliance.

This technical report examines governance thinking, principles, and approaches and applies them to the subject of enterprise security. Its primary intent is to increase awareness and understanding of the issues, opportunities, and possible approaches related to treating security as a governance concern. In addition, this report identifies resources for enterprise security that leaders can use both within their organizations and with their networked partners, suppliers, and customers.

1 Introduction

In today's economic, political, and social environment, addressing security is becoming a core necessity for most, if not all, organizations.[6] Customers are demanding it as concerns about privacy and identity theft rise. Business partners, suppliers, and vendors are requiring it from one another, particularly when providing mutual network and information access. Espionage through the use of networks to gain competitive intelligence and to extort organizations is becoming more prevalent. National and international regulations are calling for organizations (and their leaders) to demonstrate due care with respect to security.

An organization's ability to take advantage of new market opportunities directly, and through outsourcing and offshoring, often depends on available, secure network connectivity and services, and the ability to protect information and the environment within which it resides.

A wide range of current and pending U.S., national, and international legislation calls for organizational leaders to demonstrate an acceptable standard of due care and to exercise due diligence[7] in how they manage their computing infrastructures and the information they store, transmit, and process. Organizations are expected to comply with an ever-growing number of standards, guidelines, checklists, and assessment and audit instruments. The U.S. federal government has recognized the potential consequences of security breaches to critical infrastructures in its *National Strategy to Secure Cyberspace,*[8] more specifically in its Federal Information Security Management Act (FISMA),[9] and in formulating cybersecurity initiatives within the Department of Homeland Security such as US-CERT.[10] According to the Corporate Governance Task Force (CGTF),[11]

> Today's economic environment demands that enterprises in both the public and private sectors reach beyond traditional boundaries. Citizens, customers, educators, suppliers, investors, and other partners are all demanding better custodianship of their information and more access to strategic resources. As enterprises rise to meet this

[6] The terms "organization" and "enterprise" are intended to convey the same meaning and used interchangeably throughout this report.

[7] "A legally recognized duty can arise in various ways. It can arise from a statutory obligation. It can be created by a contract or promise. It can be assumed in language found in an institutional policy or mission statement. It can be implied from control of facilities or from a special relationship between the parties. It can be implied by the standard of care in the industry" [Tribbensee 03].

[8] http://www.whitehouse.gov/pcipb/, 2003

[9] http://csrc.nist.gov/policies/FISMA-final.pdf, 2002

[10] http://www.us-cert.gov/

[11] Convened after the National Cybersecurity Summit of 2004 [CGTF 04]. See also Appendix A.

> demand, traditional boundaries are disappearing and the premium on information security is rising. Heightened concerns about critical infrastructure protection and national homeland security are accelerating this trend [CGTF 04].

The Business Roundtable asserts the following in its report *Committed to Protecting America: CEO Guide to Security Challenges* [BRT 05]:

> Information security requires CEO attention in their individual companies and as business leaders seeking collectively to promote the development of standards for secure technology.
>
> Boards of directors should consider information security an essential element of corporate governance and a top priority for board review.

An organization's ability to achieve and, more importantly, sustain adequate security starts with executive sponsorship and commitment, catalyzed by governance actions. The board, too, has a role in governing for enterprise security. Directors can encourage and approve enterprise-wide security policies and can oversee security-policy implementation and compliance. Ultimately, the organization's directors and senior executives set the direction for how enterprise security is perceived, prioritized, managed, and implemented.

Target Audience

The primary audience for this report consists of C-level executives of major corporations,[12] both for-profit and not-for-profit, and those who hold equivalent positions in government agencies and academic institutions. More specifically, the core target audience for this report is likely to comprise chief information officers (CIO), chief security officers (CSO), and chief information security officers (CISO). We expect that members of governing bodies such as boards of directors as well as leaders of board committees such as the audit committee may also find this report useful.

The secondary audience for this report includes those responsible for security who communicate on this subject to members of the primary audience, and those who support officers in fulfilling their governance responsibilities.

Desired Outcome

Our desired outcomes for this report are increased awareness and understanding, and to encourage action to address security at an enterprise level and as a governance concern. Our work in determining the extent to which security needs to be a governance concern is applied-research work in progress that benefits from communication, feedback, and community involvement. To realize these outcomes and benefits, we hope for the following response from readers of this report:

[12] Refer to Appendix C for titles of officers who are members of the primary audience for this report.

- requests to share this report with their constituencies
- identification of organizations and sources working in this topic area beyond those cited, that can provide additional value, divergent perspectives, and experience reports
- interest in participating as a collaboration, benchmark, and/or case-study partner

Why is the CERT®[13] Program at the Software Engineering Institute interested in this topic?

In almost all of the SEI's work in software engineering improvement, we find that executive awareness and understanding are essential to achieving and sustaining any level of improvement so that it becomes part of everyday business conduct. To achieve the CERT mission—widespread community improvement in security—we need to address this topic.

Approach

Enterprise security is important to almost all organizations. But with so many other topics vying for leadership attention, what priority should be assigned to enterprise security? What constitutes adequate security and what constitutes adequate oversight of it? How can leaders use governance to sustain adequate security in a constantly changing business, customer, risk, and technology environment?

In our work with executives, we find that one of the most constructive ways to present a new area of inquiry is as a series of questions to ask. For those in demanding positions with little time to spare, knowing the right questions to ask and the range of acceptable responses is one of the most effective means for gaining necessary insight and perspective. Such insight is often critical for choosing oversight actions and for making competent, well-informed decisions. The remaining sections of this report are organized around key questions and answers.

Section 2 describes and defines how the phrase "governing for enterprise security" is used in this report, including its constituent terms. Section 3 describes some of the key risks and opportunities to consider when determining the extent to which governance thinking and action need to be applied to security. Section 4 lays the foundation for determining how much security is enough and further expands the definition of adequate security. Section 5 presents additional issues to consider and indicators to look for in response to the question, "What are the characteristics of effective enterprise security governance?" Section 6 briefly describes future research and development approaches based on the response to this report.

The observations, recommendations, quotes, and anecdotes presented here are drawn from in-depth discussions and interviews, workshops, conference engagements, community collaboration on related topics, and work with leaders whose organizations demonstrate varying capabilities in enterprise-security governance. In addition, confirmation of beliefs,

[13] CERT is registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

behaviors, capabilities, and actions representing dimensions of a culture of security is synthesized from many of the references cited in this report and included in the bibliography.

This first introductory technical note does not provide detailed guidance on how to implement an enterprise security governance program. It does provide example guidelines for implementation and a rich set of additional resources in Appendix A and in the bibliography.

Based on community response to this report, we intend to continue this work, capturing and recommending strategies based on experience that will help organizations develop their own programs for enterprise-security governance.

2 What Is Governing for Enterprise Security?

This section defines the concept of governing for enterprise security as used in this report, and how this definition derives from more traditional definitions for corporate, enterprise, and IT governance.

Most senior executives and managers know what governance means and their responsibilities with respect to it. Our intent here is to help leaders expand their governance perspectives to include security, and incorporate enterprise-wide security thinking into their own and their organizations' day-to-day governance actions.

While these definitions apply most directly to commercial corporations, they can also be interpreted and tailored for government, education, and non-profit institutions as well as for organizations of any size.

Governance

For this report, we define "governance"[14] as setting clear expectations for the conduct (behaviors and actions) of the entity being governed, and directing, controlling, and strongly influencing the entity to achieve these expectations. It includes specifying a framework for decision making, with assigned decision rights and accountabilities, intended to consistently produce desired behaviors and actions. Governance actions create and sustain the connections among principles, policies, processes, products, people, and performance.

Governance could be simply summarized as ensuring that organizations are doing the right things and doing things right, and at the right time. We recognize that "right things" and "things right" are relative, not absolute, concepts and that they are subject to change as the organization's goals change.

Another aspect of effective governance is to ensure that the right leaders are making the right decisions targeting the right outcomes and results. Governance relies on well-informed decision making and the assurance that such decisions are routinely enacted as intended. Governance is most effective when it is systemic, woven into the culture and fabric of organizational behaviors and actions. Systemic governance is demonstrably more effective and more sustainable than governance through oversight or governance by compliance that is enforced by the board of directors under the aegis of the audit committee.

[14] The term "governance" is much used and abused of late as the panacea for post-Enron needs for corporate reform, U.S. Sarbanes-Oxley regulatory compliance, and getting IT (information technology) cost and projects under control. The term governance historically has its roots in financial control and reporting, and as a concern for boards of directors.

Corporate, Enterprise, and IT Governance

Governing for enterprise security (GES) builds on and expands commonly defined forms of governance. These include corporate governance, enterprise governance, and IT governance.

Definitions of corporate governance typically include the relationships and incentives among boards of directors (or equivalent), senior executives, shareholders, and key stakeholders intended to ensure fiscal accountability, clear responsibility, and accurate reporting. Terms used in some definitions include *probity* (complete and confirmed integrity), *due diligence*, and *standard of due care*. The board has a duty of care to request and receive timely and reliable information to govern the organization. For example, board members should be asking the audit committee and their internal auditors if sufficient security resources are in place and effectively deployed.

Corporate governance and enterprise governance overlap when the definition of corporate governance is expanded to include the "structure through which the objectives of the enterprise are set, and the means of attaining those objectives and monitoring performance are determined" [OECD 04]. Structures and means may include, for example, policies (and their corresponding standards, procedures, and guidelines), strategic and operational plans, awareness and training, risk assessments, internal controls, and audits.

IT governance consists of the actions required to align IT with enterprise objectives and ensure that IT investment decisions and performance measures demonstrate the value of IT in meeting these objectives. Appendix B provides expanded definitions of corporate, enterprise, and IT governance.

Defining the Enterprise

An enterprise is an undertaking that takes organizational form. Forms can be physical (buildings in specific geographic locations) or virtual (via network connectivity, where physical location is not as important). In this report, we use the term "enterprise" to connote both the ordinary enterprise, which has one or more fixed places of business, and the extended or virtual enterprise. A virtual enterprise comprises all of those entities with electronic access to an organization's networks and networks of other entities to which the organization has access. Examples include an organization and all of its supply-chain partners (and their partners); and an organization and all of the entities to which it has outsourced part or all of its business processes or part or all of its supporting IT infrastructure.

A core competence of virtual enterprises in particular must be the ability to re-invent and re-configure themselves. Members of a virtual enterprise are always coming and going as business opportunities and needs dictate. This requires skill in finding the right partners, forming relationships, negotiating ground rules, putting processes in place for steady-state operation, performing to objectives, completing work, and terminating the relationship or reconstituting the relationship for the next opportunity. With respect to network connectivity, virtual enterprises must put protection strategies in place for both permeable network

boundaries (based on levels of trust) and more proximate perimeter controls (such as host-based firewalls and intrusion-detection systems) around critical systems and applications.

Those conducting business in both physical and virtual enterprises often need to be competent in dealing with cultural, linguistic, geographical, legal, and political diversity in their staffs, customers, partners, and sourcing relationships. Processes such as access control, authentication, and information handling become increasingly important and complex as they are affected by this diversity.

Enterprise Security

Enterprise security in its broadest sense comprises all organizational actions required to ensure freedom from danger and risk and precautions taken to guard against crime, attack, sabotage, espionage, accidents, and failures.[15] Topics that fit within this subject typically include fraud, loss prevention and detection, physical security, investigations, surveillance, executive and personnel protection, business continuity, disaster recovery, information/cyber security, and possibly privacy and safety. This report does not cover all of these. It focuses on those aspects of enterprise security that protect the security of information in all of its forms (electronic, physical) and the security of the systems and networks where information is stored, accessed, processed, and transmitted. The term "enterprise security" is used instead of the more narrowly interpreted "information security" to convey the need to secure information at an enterprise level, both strategically and tactically.[16]

Enterprise Security Governance

What does it mean to govern for enterprise security or, stated differently, to govern an organization to achieve and sustain an acceptable or adequate level of security?

Our definition of governing for enterprise security (GES) is

> *Directing and controlling an organization to establish and sustain a culture of security in the organization's conduct (beliefs, behaviors, capabilities, and actions).*[17]
>
> *Governing for enterprise security means viewing adequate security as a non-negotiable requirement of being in business.*

Our definition of adequate security is

---

[15] Informed by *Random House Dictionary of the English Language*, Second Edition Unabridged, 1987.

[16] As a community, we continually attempt to qualify what type of security we're describing-information, cyber, e-commerce, IT, network, and system. We'll know that we've been successful in treating security as an enterprise concern when we no longer need the qualifier [Slater 05].

[17] The Organisation for Economic Co-operation and Development (OECD) discusses the need to develop a "culture of security" in its *Guidelines for the Security of Information Systems and Networks* [OECD 02].

The condition where the protection strategies for an organization's critical assets and business processes are commensurate with the organization's risk appetite and risk tolerances.[18]

If they aren't doing so already, leaders need to treat security as a business issue. Their behaviors and actions with respect to security influence the rest of the organization. When staff members see the board and executive team giving time and attention to security, they know that security is something worth their time and attention. Directing and controlling an organization to establish and sustain a security-conscious culture is good governance.

As one small example, consider the executive who does not want to be bothered with enabling the desktop screen lockout when leaving the office (which is also automatically engaged after 10 minutes of idle time) and perform the actions necessary to log back in when returning. The executive contacts IT and tells them to continue to enforce this policy for everyone else but to disable it for the executive's desktop and laptop systems. Naturally word of this gets around and reinforces a notion that senior managers do not consider themselves subject to the same policy as everyone else. The influence of this simple act on compliance is immediate and hard to recover from because of the violation of trust and loss of credibility. Permitting exceptions to basic controls is detrimental to achieving a culture of security.[19]

Rhonda MacLean, chief information security officer, Bank of America, describes the bank's approach to enterprise security at both a governance and management level as follows [McCollum 04]:

> On a structural level, Bank of America has established a security compliance framework that includes commitment and accountability, policies and procedures, controls and supervision, regulatory oversight, monitoring, training and awareness, and reporting. Bank of America has also established a four-level information security governance model that maps out the responsibilities of board directors, business executives, chief information officers, corporate audit, the security department, legal, corporate and line-of-business privacy, and supply chain management.
>
> The board of directors is responsible for reviewing the corporate information security program and policy, while senior management is accountable for ensuring compliance with applicable laws, regulations, and guidelines and for establishing compliance roles, accountabilities, performance expectations, and metrics. It's up to the auditors to ensure the commitment and accountability for information security controls.
>
> Bank of America's corporate information security department focuses on people, technology, and processes using a protect/detect/respond-recover model and measures its progress based on the Six Sigma quality methodology. Bank of America measures security based on failed customer interactions rather than on downtime, performance, or

[18] Risk appetite and risk tolerance are defined by The Committee of Sponsoring Organizations of the Treadway Commission (COSO) in its *Enterprise Risk Management – Integrated Framework* [COSO 04].

[19] Interview with CISO, March 2005.

the number of infections or attacks. Achieving 99 percent uptime isn't important if the one percent downtime impacts 30 million customers.

In the absence of some type of meaningful governance structure and way of measuring enterprise security, the following questions naturally arise:

- How can an organization know what its greatest security risk exposures are?
- How can an organization know if it is secure enough to
  - detect and prevent security events requiring business-continuity, crisis-management, and disaster-recovery actions?
  - protect stakeholder interests and meet stakeholder expectations?
  - ensure enterprise viability?

The role of boards of directors, senior executives, and indeed all managers includes establishing and reinforcing the business need for effective enterprise security. Business objectives guide and drive actions needed to govern for enterprise security. The connection to business objectives is evident from a list of organizational assets that can be negatively affected if security governance is performed poorly such as those described in Section 3 (trust, reputation, brand, stakeholder value, customer retention, etc.). Organizations are much more competent in addressing this subject if their leaders treat the governance of enterprise security as essential to their business and are aware and knowledgeable about the issues.

As a logical extension, not only will organizations benefit individually and collectively from increased enterprise security, but ultimately, nations as a whole will benefit.[20] "The critical information infrastructures comprising cyberspace provide the backbone for many activities essential to the transaction of domestic and international business, the operation of government, and the security of a nation" [BRT 04].

The next section makes the connections among enterprise risk, enterprise security risk, and security strategy. It describes some of the key risks, challenges, opportunities, and barriers to consider when determining the extent to which governance thinking and action should be applied to security.

[20] Imagine a situation in which organizations in a specific country do not treat security as a strategic governance issue, particularly those providing critical infrastructure support (telecommunications, electrical power systems, gas and oil storage and transportation, banking and finance, transportation, water supply systems, emergency services, continuity of government) [CRS 04c]. It is conceivable that instead of enjoying long-term national prosperity, a nation could, as one consequence, see the flight of capital to countries with a better, or at least more acceptable, risk/reward ratio with respect to critical infrastructure protection [Spafford 05].

3 What Are the Risks and Opportunities?

3.1 Enterprise Risk and Enterprise Security Risk

Governance and risk management are inextricably linked, with governance action being an expression of responsible risk management and effective risk management requiring efficient governance.[21] Inserting security into ongoing governance and risk management conversations is an effective and sustainable approach for enterprise-wide security governance.

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) defines risk as "the possibility that an event will occur and adversely affect the achievement of objectives" [COSO 04].

COSO discusses enterprise risk management as follows:

> All entities face uncertainty, and the challenge for management is to determine how much uncertainty it is prepared to accept as it strives to grow stakeholder value. Enterprise risk management enables management to identify, assess, and manage risks in the face of uncertainty, and is integral to value creation and preservation. Enterprise risk management is a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise. It is designed to identify potential events that may affect the entity, and manage risk to be within the entity's risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.

Enterprise risks within the scope of this report include financial (including credit), legal and compliance, operational,[22] market, strategic, information, technology, personnel, and reputation. Enterprise security risks that derive from these may include those that damage stakeholder trust and confidence, affect customer retention and growth, violate customer and partner identity and privacy, disrupt the ability to offer and fulfill business transactions, adversely affect health and cause loss of life (for example, in the case of improper handling of medical records and patient information), and adversely affect the operations of national critical infrastructures.

[21] Historically, corporate governance has involved gaining access to capital, whether for growth, operations, or other needs.

[22] According to Basel II (the capital adequacy framework described at http://www.bis.org/publ/bcbs107.htm), operational risks are risks of loss resulting from inadequate or failed internal processes, people, and systems or from external events.

While this report focuses primarily on the negative consequences resulting from realized security risks, organizations might also consider how investment in security can enable an organization to act on new opportunities to better achieve business objectives. These may include

- enabling new types of products and services
- communicating with customers in a reliable, cost-effective, and timely manner
- causing transactions to occur with greater integrity and privacy, thus ensuring business throughput, customer satisfaction, and customer confidence, which can all help create and sustain customer loyalty
- enabling new types of customer/supplier engagement; interacting in a more timely and reliable way with the organization's supply chain
- providing more secure access by internal and external staff to enterprise applications

An organization's ability to take advantage of new opportunities often depends on having open, accessible, available, and secure network connectivity and services, balanced with adequate security controls.[23]

For example, if an organization diligently protects a customer's personal information, privacy, and identity, and if the customer knows this through experience of doing business with the organization, the customer is more likely to increase the number of Internet-based interactions. Transactions may include purchasing products and services and using help and customer assistance online (assuming that these are offered in an understandable and user-friendly manner), instead of placing a phone call or visiting a physical location. In most cases, transactions can be accomplished quickly with little to no requirement for human interaction, resulting in cost and time savings for both parties.

Establishing and maintaining confidence in an organization's security and privacy posture increase the likelihood that customers will refer others to the products and services offered by that organization.

3.2 Security Strategy Questions

Determining the range of actions that an organization needs to take to reduce security risk to an adequate or acceptable level depends on what an organization needs to *protect* and what it needs to *prevent*. Consider the following questions from an enterprise perspective:

- What needs to be protected? Why does it need to be protected? What happens if it is not protected?
- What potential adverse conditions and consequences need to be prevented? At what cost?

[23] "The ability to quickly and reliably share information is key to the long-term success of any venture. But wrestling with the potential tradeoffs between speed and collaboration vs. risk and exposure is not a simple matter, especially in an increasingly complex regulatory environment" (http://mba.tuck.dartmouth.edu/digital/Programs/CorporateRoundtables.html).

- How much disruption can we stand before we take action?
- How do we determine and effectively manage residual risk (the risk remaining after mitigation actions are taken)?

Clearly an organization cannot protect and prevent everything. Interaction with key stakeholders is essential to determine the organization's ability to tolerate risk and appetite to tolerate the impact if the risk is realized. In effect, security as a component of risk management involves a process of determining what could go wrong, the likelihood of such an event occurring, the impact if it did, and actions to mitigate or minimize both the likelihood and the impact to an acceptable level (risk appetite) with an acceptable range of variation (risk tolerance).

The answers to these questions can help organizations determine how much to invest, where to invest, and how fast to invest in security-governance actions. They serve as one means to identify security risks to the enterprise and quantify the degree of risk exposure. In the absence of answers to these questions (and a process for periodically reviewing and updating them), an organization may find it difficult to define and deploy an effective security strategy and thus unable to effectively govern for enterprise security.[24]

The following sections describe some of the challenges, opportunities, risks, and barriers that should be considered in crafting an effective enterprise-security governance program.

3.3 Trust

Achieving and preserving trust are among the most essential outcomes of governing for enterprise security. Regarding trust, Larry Ponemon writes that

> The trusted enterprise is an organization embracing a set of corporate values and behaviors that guide all business practices. It is a highly ethical organization that treats its customers, employees, partners, and shareholders with respect and stewardship. The CEO and board are deeply engaged in managing the organization's operating risk in a way that delivers maximum value in a safe and secure environment [Ponemon 04].

Dan Geer states

> The central truth is that information security is a means, not an end. Information security serves the end of trust. Trust is efficient, both in business and in life; and misplaced trust is ruinous, both in business and in life. Trust makes it possible to proceed where proof is lacking. As an end, trust is worth the price. Without trust, information is largely useless [Geer 04a].

[24] Refer to *Managing Information Security Risks: The OCTAVE Approach* [Alberts 02] for more information on this subject.

Citigroup and OnStar are so serious about security that they invest in making it part of their brand image. Citigroup wants to be known as the company that rapidly detects fraud and helps its customers deal with identify theft in its credit card business. OnStar advertises its ability to provide a reliable and compassionate intermediary between a consumer in trouble and third-party service providers such as the fire department, paramedics, and law enforcement, providing peace of mind in an emergency [Wheatley 04]. Most financial services and insurance firms consider themselves to be in the trust business, and thus appreciate the value of building and preserving trust as the most critical success factor. Here is another quote from Dan Geer:

> In terms of valuing information, instead of asking "How much is your brand worth?" ask, "Knowing what you know now and starting from scratch today, how much money and time would it take to build a brand as good as the one you have now?" You can get a sense of what information enables by looking at what the absence of that information disables, leading to insights on the appropriate level of protection [Geer 04b].

Trust is an essential element of protecting customers and their information, protecting market share, sustaining market and customer confidence, increasing stock price, preserving reputation, and enhancing an organization's brand. Trust is hard to build and easy to lose in the face of a public breach of security or customer privacy. Just consider companies enjoying headline attention as their customer databases are compromised, raising widespread concerns about identity theft. Some are finding that regaining trust once lost may not be possible.

An increasing number of organizations understand the inextricable link between trust and security in today's globally connected environment. One interviewed CISO states "Security is a necessary consideration in everything that we do. We need to protect customers and employees. We are the custodian for a lot of information that belongs to other people."

The relationship between trust and security requires that governance thinking and action be applied to security risk management and investment decisions. One way to consider valuing investments in enterprise security is to include them on the organization's financial statement as goodwill.[25] Enhancing brand and trust by building and preserving security requires governance-level action.

3.4 Stakeholder Value

Every organizational entity survives and thrives by creating value for its stakeholders. Value is created, preserved, or eroded by leadership decisions and actions, from strategy to day-to-

[25] For accounting purposes, goodwill is an intangible asset valued according to the advantage or reputation a business has acquired over and above its tangible asset. Any factor that translates into the organization's ability to increase its earning power (or ability to accomplish its mission) can contribute to goodwill, such as its reputation, customer service, and perhaps its ability to adapt to changing risk environments [Caralli 04c].

day operations. Leaders understand that they are accountable for protecting stakeholder interests in a demonstrable manner as part of responsible enterprise governance.

Stakeholders may include regulators, shareholders, investors, rating agencies, partners, suppliers, vendors, customers, employees, consultants, governments (local, state, and national), surrounding communities, citizens, and other communities of interest such as certifying bodies and professional associations. From the perspective of enterprise security, stakeholder interests are likely to include

- accurate reporting of the returns, effectiveness, and productivity of the enterprise
- creation, preservation, and enhancement of the organization's reputation
- availability and reliability of services (business resilience)
- demonstrated due diligence with respect to protecting against malicious attacks (internal and external) and accidents that can be anticipated
- ensuring of only authorized access to enterprise information
- protection of the privacy of stakeholder information

Stakeholder interests are most effectively protected by selecting a broad set of enterprise security principles (refer to Section 5.3), interpreting and tailoring these for the enterprise, and ensuring their use and enforcement in the normal course of business. These actions help to ensure that an organization achieves and sustains a culture of security.

3.5 Ethics and Duty of Care

Given the growing marketplace demands for integrity, transparency, and responsible oversight, demonstrating ethical and socially conscious behavior is becoming a required core competence for many organizations. Organizations must safeguard customer information and use information, systems, and networks in a way that satisfies widely agreed-upon expectations. These expectations are established by social norms, obligations, norms for responsible Internet citizenship, and enterprise codes of ethical conduct. Policies describing the ethical use of information need to address ownership, privacy, and the risk of using information and systems to the detriment of an enterprise and its stakeholders. Stakeholders are becoming more educated, understanding the extent to which their action or inaction may harm others, understanding the consequences of unethical behavior, and demanding that the legitimate interests of others be respected.

Protecting stakeholder interests includes responsible behavior when connecting enterprise networks to the global internet. The Institute of Internal Auditors states

> In the modern world, everything business or government does with their information technology becomes part of the global information infrastructure. We must build infrastructure to a very high standard. Attaching weak components to the infrastructure puts your organization as well as your neighbors at risk. Responsible citizens will contribute only sound components to that cooperative infrastructure [IIA 01].

Given the increase in regulatory action worldwide (see Section 3.7) and emerging case law in many countries, enterprise leaders need to fulfill their responsibilities to protect digital assets, including stakeholder information. Director and officer oversight of corporate digital security is embedded within the fiduciary duty of care owed to company shareholders. Under common law as interpreted by U.S. state courts [Westby 04], such oversight may include:

- governing business operations to ensure protection of critical information assets
- protection of market share, stock price, and reputation dependent on digital assets
- governing employee conduct through training and security-policy enforcement
- ensuring that compliance requirements are met

To fulfill their duty of care under current U.S. regulations, directors must exercise a level of care that a reasonably prudent and careful person (including a director of a similar organization) would have used under similar circumstances, with negligence defined as the failure to do so [Westby 04, Braun 04]. Directors who make their decisions with due care and in good faith, and without conflict of interest, may receive protection for their decisions under the judicial principle called the Business Judgment Rule.[26] Standards for information security rank high among the issues worthy of attention at this level [Lajoux 05]. Taking effective and demonstrable action to protect critical information assets is a means for directors to demonstrate that they are acting in a reasonable[27] manner.

It may be useful for an organization to view its computing networks as the organization's nervous and circulatory systems, with information being the lifeblood that is created, transmitted, and stored in these systems. Useful questions to ask[28] include

- What responsibility does an enterprise have for protecting the information in its computer systems, particularly information that belongs to others?
- What responsibility does an enterprise have to keep its information systems from being used to harm others?
- What are the organization's worst-case scenarios for security compromise? Most likely scenarios?

As these questions are answered, they will help define an evolving enterprise-security minimum standard of due care that will serve to establish, at any point in time, a definition of what constitutes an adequate or appropriate level of security.

---

[26] See also *Cyber Security & Corporate Liability* [Zeichner 03].

[27] The standard of what is reasonable evolves as organizations become more aware of the issues and establish controls (i.e., as the practice becomes more mature). The evolution of what constitutes prudent or acceptable behavior argues for organizations to revisit their decisions about risk and deployed controls periodically to ensure that they continue to achieve and maintain an acceptable level [Gerdes 05].

[28] Informed by "An Emerging Information Security Minimum Standard of Due Care" [Braun 04].

3.6 Compliance and Legal Liability

Failure to protect stakeholder interests with respect to certain categories of information or failure to prevent unauthorized access to personal information may have serious legal consequences. An enterprise-wide approach to security governance can help an organization maintain compliance with new and expanding laws and regulations and avoid legal liability related to statutory or common law.

Rather than focusing on a framework for cyber or information security, current U.S. federal legislation and related regulatory programs have focused on an interest in either of the following:

- protecting the privacy of individually identifiable information held on private computer systems
- improving private-sector oversight of financial reporting

Three current U.S. laws need to be considered when addressing security at a governance level:

- the U.S. Gramm-Leach-Bliley Act of 1999 (protecting personal information for financial-institution customers)
- the U.S. Health Insurance Portability and Accountability Act of 1996 (protecting personally identifiable health information held by certain entities
- the U.S. Sarbanes-Oxley Act of 2002 (mandating expanded public-company financial-control audits, including information security)

These laws have all provided regulatory incentives for C-level executives and boards of directors to pay closer attention to the subject of information security and thus information-security—or more broadly enterprise-security—governance. The Sarbanes-Oxley Act, more than any other current legislation, has had the greatest influence on security governance. This is because the statute makes leaders of public corporations responsible for establishing and maintaining adequate internal controls. A similar security effect derives from both state and international law. The California Database Protection Act (CA SB 1386; notification of personal security-information breaches) and European Union (EU) Directives on data protection and privacy and electronic communications are affecting multi-state and multinational organizations [CRS 05].

The U.S. Office of Management and Budget (OMB) has made eliminating vulnerable systems in government and for government contractors a direct responsibility of senior executives. The OMB demands immediate periodic reporting from all agencies on the security-configuration requirements they are implementing and the extent of implementation.

Particular care must be exercised when securing technology that supports financial-reporting processes and protecting the privacy of customer information. The absence of adequate security controls can affect organizational compliance with Sarbanes-Oxley; the U.S. Federal Information Systems Management Act (FISMA); the EU, Australian, Canadian, and Japan privacy directives; Basel II; and the California Database Protection Act requirements.

An IT-centric approach to security without adequate governance provisions can lead to omissions or commissions that, if pervasive or critical, can be considered significant deficiencies. Where key internal controls,[29] including financial controls, are affected or the organization has failed to correct significant IT-security control deficiencies identified in the preceding year (such as in patch management), management may face the possibility of having to make a formal statement of "material weaknesses" [IIA 05b].

Compliance issues related to legislative and regulatory programs and the criminal and civil liabilities that can arise from their violation are only one part of the legal-liability exposure. There remains the significant liability that can result from national/federal and state court litigation claims based on a breach of contract, tort, or property rights. Civil litigation, in which private parties, both individuals and organizations, bring causes of action before the courts, provides an effective platform for the promotion of computer security. Moreover, cybersecurity and critical-infrastructure strategies issued by the U.S. federal government in 2003 help "establish standards of security conduct and accepted notions of security risk that are likely to be applied in civil litigation" [Matsuura 03].

Governing for enterprise security ensures that the accountability framework and necessary level of oversight are in place for

- the informed selection and implementation of effective security controls
- their application to information and information systems
- regular reporting on the effectiveness of these controls

We recommend an enterprise-wide approach to security to ensure that these controls are adequately identified, architected, implemented, and tested in conjunction with all other internal controls and in concert with both internal and external audits. In our experience, this is the most effective path for mitigating risks associated with the liability exposures described in this section.

3.7 Customer and Partner Identity and Privacy

Concerns about the risks associated with personal privacy and identity are growing. Violations of these and their constituent costs, legal consequences, and effects on reputation and stock price are regularly reported in the media. A typical example states, "The Federal Trade Commission estimates that approximately 3,000,000 Americans were the victims of identify theft in 2002. A business that obtains consumers' personal information has a legal duty to ensure that the use and handling of that data complies in all respects with representations made about the company's information-security and privacy practices" [Braun 04].

---

[29] "Over the decades, the U.S. Securities and Exchange Commission (SEC) has ruled that internal controls include policies, procedures, training programs, and processes other than financial controls. The SEC has clearly defined internal controls to include the 'safeguarding of assets against unauthorized acquisition, use, or disposition'" [Tarantino 04].

The impact of disclosure of personal information that had been entrusted to an organization on that organization's reputation can be profound. Leaders should ask, "How much is our reputation worth?" Once lost, reputation can be difficult to get back [Charette 05].

As identity theft and related violations of privacy become more prevalent, public backlash from both consumers and legislators could be significant. Increasingly, consumers and business partners expect that a certain level of standard security practice should be in place in any competent organization. This expected level of standard practice is likely to continue to escalate. However, reputation need not be considered solely in negative terms. Leaders should also ask, "How much is it worth for us to be seen by our customers and business partners to be actively concerned with safeguarding their information?" Proactive approaches to security can enhance an organization's reputation as a trusted partner [Charette 05].

International privacy regulations such as those in the European Union (EU), Japan, and Australia are more stringent than their U.S. counterparts, so approaches to comply with such regulations must be developed with proper appreciation of country or regional requirements [Gartner 04].

> Privacy compliance is an extremely complex endeavor in which business risk decisions are paramount. The EU has the strictest privacy laws (although Hong Kong and New Zealand also have strict laws), and legal risks are highest in Europe. However, not all enterprises will face equal risk. Compliance with and enforcement of the implementation of the EU Data Protection Directive (DPD) across EU member states have been minimal at best. Data protection authorities have mainly pursued the most egregious offenders. In addition, non-EU enterprises, especially consumer or technology companies, have attracted the attention of some data protection authorities because healthcare, pharmaceutical, and financial services companies face greater customer privacy concerns.

U.S. or multinational companies should be especially wary of how they treat EU employee data and how they monitor EU employees' electronic activities. EU employee tribunals are common, and EU employees frequently take their employers to court.

Organizations are increasingly finding that implementing a global approach with respect to privacy can meet the majority of national or regional privacy requirements, providing some opportunity for cost containment through standardization.

Almost all organizations collect, process, store, disseminate, and transfer customer information in some form, most likely digital. Protecting such information and preventing actions that can cause unintended disclosure and use are increasingly required to meet legal requirements and preserve customer trust. Given the business implications, these actions should be evaluated and governed enterprise-wide as part of a comprehensive security program.

3.8 Ability to Offer and Fulfill Business Transactions

The Internet has equalized access to information world wide. Risks and opportunities increasingly derive from who you are connected to and who is connected to you rather than from where you are physically located. Because of the ready and direct access they have to those with whom they wish to transact business, and the ease with which they can change these choices for any reason, today's marketplace is driven by consumers. Sometimes the needs and requirements of consumers are different from or even at odds with the identified or stated needs and requirements of the business.

An organization's ability to competently offer and fulfill business transactions is most visible to the customer. Making items of interest easy to find quickly and conveniently with accurate and competitive pricing, with immediate order confirmation, and with timely delivery contribute to the growth of Internet-based business. A good example of how security enables business transactions is online banking. A bank customer can be confidently assured of a secure flow of funds via an Internet connection, rather than having to find an open bank branch in a foreign city at 4:00 a.m. [McMillan 05].

> Information security is to the economy of tomorrow what contract law is to the economy of today. It extends trust and thus enables economies to expand. A robust economy is one in which transaction costs—discovery, negotiation, arbitrage, settlement, and adjudication—are, in the broadest sense, low. The Internet and the electronic commerce it enables have low transaction costs compared with their predecessors. However, the nature of electronic communication is that it is location-independent, essentially instantaneous, and—unless modified—anonymous [Geer 04a].

Here we have another example of the opportunity and the risk as a result of transacting business on the Internet. A security-conscious organization considers all aspects of its transaction-handling processes as part of its approach to enterprise-security governance.

3.9 Barriers to Consider

This section identifies several pervasive barriers that often make enterprise security a daunting undertaking, requiring tenacity and perseverance. When effectively overcome, these barriers can also represent opportunities that may reduce the potential for loss, preserve and enhance business value, and create marketplace advantage.

We know that security is hard, often annoying, and something most people wish they didn't have to deal with, as individuals and in their organizations. There are formidable disincentives to addressing security at more than just a tactical, technical level. As a networked community, we don't fully understand what it means to put an effective security program in place, and there are no reliable measures and benchmarks for knowing if we've done enough. Achieving a particular state of security is no guarantee that it can be sustained. Achieving security is not a one-time project with a beginning and an end. It requires

continuous monitoring, improvement, and thus, attention and investment, and security investments often come at the expense of something else.

Attending to security at the enterprise level is often hard to justify. For those responsible for security, it is often difficult to persuade senior executives and boards of the need to implement enterprise security in a systemic way. For most organizations and for most people, security is an abstract concept, concerned with hypothetical events that may never occur. In this respect, it often has some of the same characteristics as insurance.

Security cannot be contained or delegated to a specific function or department within an organization. Although many have treated it as such, missing constituent elements of people and process, security is not just a technical problem. Many functions and departments within the organization need to interact to create and sustain an effective security solution that includes technological, organizational, regulatory, economic, and social aspects.

Security is sometimes described as an emergent property of both networks and the organizations they support. What this means is that the precise location where security is enacted cannot be identified, as its condition is often reflected in the intersections and interactions of people, process, and technology. As the organization and the underlying network infrastructure change in response to the changing risk environment within which each exists, so will the security state. Effective security can be thought of as an attribute or characteristic of an organization. It becomes evident when everyone gets involved, creating a culture of security that displaces ignorance and apathy.

There are no widely accepted (de facto or de jure) standards of best practice (with the possible exception of ISO 17799 [ISO 00b]), metrics for characterizing security performance against some measure of adequacy, or industry-accepted benchmarks. However, there is an ever-growing number of guidelines and checklists that identify practices that are considered acceptable by most professionals, thus passing the test of reasonable practice. The Internet's cybersecurity state today is far worse than what it would be if generally accepted practices were properly deployed to address known problems. This is evidenced by the number of vulnerabilities reported to the CERT Coordination Center (CERT/CC),[30] many of which have known solutions that have not been implemented. This is particularly alarming for national critical infrastructures such as telecommunications, transportation, banking and finance, and electric, oil and gas, and water distribution. Clearly, the existence of accepted sets of commonly used good practices and metrics do not guarantee widespread use.

Actions taken to secure an organization's assets and processes are typically viewed as disaster-preventing rather than payoff-producing (again, like insurance), which makes it difficult to determine how best to justify investing in security, and to what level.

Benefits of investing in security are often seen only in events that do not happen. As it is impossible to prove a negative, what value does an organization place on cost avoidance?

[30] http://www.cert.org/stats/cert_stats.html

This same difficulty has dogged efforts to improve software quality, conduct proper testing, keep documentation up to date, maintain current configuration and hardware/software inventory records, etc. [Braithwaite 02]. Unlike insurance where the causes of loss are essentially known or change very slowly, the nature of what is considered a security threat and the number and type of vulnerabilities affecting information and systems are constantly evolving and changing.

Furthermore, installing security safeguards is often seen as having negative consequences such as added cost; diminished application, system, and network performance; and user inconvenience (for example, multiple means for authentication that change regularly and are hard to remember). "While internal auditors often identify vulnerabilities within a business system, their recommendations for more stringent system controls are in many cases overruled because of direct costs of implementing and maintaining those controls or because they introduce unwelcome inefficiencies" [Taylor 04a].

This situation is difficult to improve without a significant increase in the reporting of incident cost/loss metrics to extrapolate actual conditions or estimate probable results that would have occurred had certain steps not been taken to reduce the exposures. This is analogous to insurance actuarial data that provides a statistical basis for estimates of loss [Gerdes 05].

In short, security is hard to define and implement. Security is not supported by a universal standard, can be seen as having negative impacts such as cost and inconvenience when implemented, and is usually seen as—at best—avoiding disaster or business impact (cost) rather than providing benefit and competitive advantage. An effective approach to governing for enterprise security must confront these barriers head on, offering counterpoints and benefits to anticipate and offset each barrier. Increasing the awareness, knowledge, and understanding of security in an organization is a necessary first step to changing common beliefs.

The next section provides definitions and guidelines for determining what constitutes an adequate or appropriate level of security at the enterprise level.

4 How Much Security Is Enough?

CIOs, CSOs, and system administrators may dream about achieving a state of complete organizational security, but pragmatically they realize this is unrealistic and financially imprudent. However, it is feasible to adopt the concept of achieving *adequate security* at an enterprise level in response to the question, "How much security is enough?"

Achieving adequate security means more than complying with regulations or implementing commonly accepted best practices. Formulating the concept of adequate security helps define the benefit and optimized outcome for security investment. This formulation must occur in the context of identifying and managing the security risks to an organization's mission and objectives.

One approach to defining an adequate or appropriate level of security is to compare and contrast it with a theoretical state of absolute security—an ideal condition where *all* security requirements[31] for critical business processes and assets are satisfied (assuming that an organization has identified these as worthy investments).

So, in this context, how might we define and determine adequate security, recognizing that

- absolute security is not only impossible but highly undesirable from effectiveness, efficiency, risk/reward, and cost/benefit perspectives
- governing security at an adequate or appropriate level enables enterprise risk to be managed in a cost-effective manner

4.1 Characteristics to Consider

Security-conscious leaders evaluate how much and in what ways their enterprise depends on Internet connectivity, IT infrastructure, and electronic assets for business performance and continuity. They are able to better determine the degree to which governance decisions should take the security of such assets into account. Factors that can aid in making this determination are described below.[32] Together with a comprehensive risk assessment, an aggregation of these factors can form a repeatable basis for security-investment decisions.

Organization Characteristics

- Size (number of physical locations, employees, and customers; level of revenue)

[31] Security requirements typically include preserving appropriate levels of confidentiality, availability, and integrity.

[32] These factors are derived from [CTGF 04], based on original work reflected in [TechNet 03]. Refer to the TechNet evaluation to see one application of these factors.

- Complexity (organizational units, products, services, processes, systems, structure—for example, centralized or decentralized, co-sourcing and outsourcing relationships, external supply-chain partners)
- Value and criticality of the organization's intellectual property, particularly information stored or transmitted in electronic form
- Dependence on IT systems and the Internet to offer products and services to customers
- Impact from system downtime or a disruption of Internet connectivity on the organization
- Impact of system, administrative, or transactional errors on the organization
- Degree and rate of change within the organization (expansions, mergers, acquisitions, divestitures, new markets, etc.)
- Dependence on multinational operations
- Plans for transnational operations (internal functions transferred offshore or outsourced to offshore locations, geographical expansion into areas representing increased revenue)

Market Sector Characteristics

- Potential impact to national, international, or critical infrastructures as a result of outages or interruptions in organizational systems
- Customer sensitivity to and expectations for security and privacy
- Level of sector regulation that pertains to security (refer to Section 3.7)
- Potential brand and reputation damage of a publicly disclosed security incident or violation of customer privacy
- Extent of enterprise operations that depend on third parties (partners, contractors, suppliers, vendors) and connectivity with third-party networks
- Customers' ability and likelihood to quickly switch to a competitor, based on competitor's ability to offer more secure, reliable services
- Extent to which the organization does business in a geographically or politically sensitive area where it could be a likely target of damaging physical or cyber attack

4.2 Defining Adequate Security

Determining adequate security is largely synonymous with determining and managing risk. Where possible, an organization implements controls that satisfy the security requirements for its critical business processes and assets. Where this is not possible, security risks to such processes and assets are identified, mitigated, and managed at a level of residual risk that is acceptable to the organization.

As described in Section 3.2, determining adequate security depends on what an organization needs to protect and what it needs to prevent to support achievement of enterprise objectives. Selecting protection and prevention actions based on risk helps determine how much to invest, where to invest it, and how fast.

We define adequate security as

> *The condition where the protection strategies for an organization's critical assets and business processes are commensurate with the organization's risk appetite and risk tolerances.*

Protection strategies include principles (as described in Section 6.3), policies, procedures, processes, practices, and performance indicators and measures, all elements of an overall system of controls.[33]

An *asset* is anything of value to an organization. Assets include information such as enterprise strategies and plans, product information, and customer information; technology such as hardware, software, and IT-based services; and supporting assets such as facilities and utilities. Critical assets are those that directly affect the ability of the organization to meet its objectives and fulfill its critical success factors [Caralli 04a]. As stated earlier, assets also include items of significant yet largely intangible value, such as brand, image, and reputation.

A *process* is a systematic series of progressive and interdependent actions or steps by which a defined end result is obtained. Business processes create the products and services that an organization offers and can include customer relationship management, financial management and reporting, and management of relationships and contractual agreements with partners, suppliers, and contractors.

Risk appetite is defined by COSO as ". . . the amount of risk, on a broad level, an entity is willing to accept in pursuit of value (and its mission)." Risk appetite influences the entity's culture, operating style, strategies, resource allocation, and infrastructure [COSO 04]. Risk appetite is not a constant; it is influenced by and must adapt to changes in the environment.

Defining the organization's risk appetite is an executive responsibility. It is undertaken in conjunction with evaluating alternative business models in pursuit of the organization's goals and objectives. Management assesses the alternatives, sets objectives aligned with strategy, develops business processes to accomplish the plan, and manages any inherent risks. Risk appetite can be expressed as impact (potential consequences of a risk-based event), likelihood of a risk's occurrence, and associated mitigating actions [Carey 05]. For identified and evaluated risks, risk appetite could be defined as the residual risk the organization is willing to accept as the default condition of having implemented its set of risk-mitigation and monitoring processes [Taylor 04b].

Risk tolerances are defined by COSO as ". . . the acceptable levels of variation relative to the achievement of objectives, [which] are often best measured in the same units as the related objectives" [COSO 04]. In defining acceptable levels of variation, risk tolerance defines and

[33] A system of internal controls often includes categories such as administrative, technical, and physical as well as directive, preventive, compensating, detective, and corrective (http://www.nysscpa.org/cpajournal/2003/0103/features/f013603.htm).

delineates the range of impact and corresponding risk to the organization. This is embodied in defining and using impact and risk-evaluation criteria, which can be expressed both qualitatively and quantitatively.

Risk tolerance could be defined as the residual risk the organization is willing to accept after implementing risk-mitigation and monitoring processes and controls. One way to implement this is to define high, medium, and low levels of residual risk. An example is a policy to conduct prioritized mitigation for high- and medium-level risks and to accept (monitor) low-level risks as the default condition.

With risk appetite and risk tolerances defined,[34] how does the organization manage different levels of inherent and residual risk? How does an organization prioritize risks requiring mitigating actions? In quantitative terms, what "value at risk" is acceptable [Taylor 04b]?

Consider the following example: A retailer decides to enter the e-commerce marketplace but has a low risk appetite relative to its relationship with existing customers, particularly with respect to fulfilling orders promptly and accurately. To protect these relationships, management allocates necessary resources (people, processes, technology) to ensure that (1) order-to-delivery response times meet or exceed defined targets and (2) order-fulfillment accuracy meets or exceeds defined criteria. Management is now conducting business online and has installed the resources needed to protect its reputation for timely and accurate fulfillment of customer orders. It has set a target for delivery within seven days of accepting orders and has guaranteed delivery within two weeks by a statement on its Web site. However, how much variation is management willing to tolerate with respect to delivery and order-accuracy targets? Is a five-day average variance around the delivery target too much? The level of variation relative to achievement of objectives is known as the risk tolerance [Taylor 04b].

4.3 Determining Adequate Security

With the benefit of this description, a useful way to address the question "How much security is enough?" is to first ask "What is our definition of adequate security?" by exploring the following more detailed questions:

1. What are the critical assets and business processes that support achieving our organizational goals? What is the organization's risk tolerances and risk appetite, in general and with respect to these assets and processes?

[34] To further clarify risk appetite and risk tolerances, Moulton and Coles [Moulton 03] define enterprise pain threshold as "The financial or other indicator point at which the executive management of the enterprise will, or should, know that the loss or damage caused by an event, including a control failure related to loss limitation or mitigation for the event, would be of sufficient magnitude to put the enterprise at risk; and, could consequently result in their being held personally accountable by shareholders and/or regulators."

2. Under what conditions and with what likelihood are assets and processes at risk? What are the possible adverse consequences if a risk is realized? Do these risks fit within our risk appetite and risk tolerances?
3. In the cases where risks are beyond these thresholds, what actions do we need to take to mitigate and with what priority? Are we making conscious decisions to accept levels of risk exposure and then effectively managing residual risk? Have we considered mechanisms for sharing potential risk impact (for example, through insurance or with third parties)?
4. For those risks we are unwilling or unable to accept, what protection strategies do we need to put in place? What is the cost/benefit or return on investment of deploying these strategies?
5. How well are we managing our security state today? How well will we manage our security state 30 days, 6 months, and a year from now? Are we updating our understanding and definition of our security state as part of normal planning and review processes?

Example

One of Acme, Inc.'s critical *assets* is the customer-transaction database, which includes order history. This is used actively in targeted marketing and sales *processes* with exceptional results (repeat sales). It has taken three years of staff effort to build and populate this database at an estimated cost of USD $1 million. Ongoing operations and maintenance costs including the protection strategies described below are USD $200,000.

There are specific events, impacts, and consequences that Acme needs to prevent. Competitors regularly attempt to obtain access to this information or to obtain a copy of this information (high risk). Management is sensitive to the risk of disclosure by sales and marketing staff who are approached by competitors to share this information for personal financial gain (medium risk). Third-party intruders have threatened to obtain access to and disclose this information on the Internet (low risk). While Acme believes it offers superior service, creating customer loyalty in the face of competitive pressure to switch, it places the value at risk at USD $10 million (*risk appetite*).

Security requirements for this asset include zero tolerance of unauthorized disclosure (violation of confidentiality), continuous validation of data integrity (by automated comparison with a trusted, securely stored version), and 99.999 percent availability (*risk tolerances*).

Protection strategies include

- principles enacted by policies and procedures that state these requirements and risk tolerances for this asset
- clear assignment of roles and responsibilities and periodic training for staff and managers involved in protecting this asset; financial incentives for those demonstrating innovative approaches to asset protection

- periodic training for staff having access to this asset; immediate removal of access and authorization for any staff member whose responsibilities no longer require a need for access, including any change in employment status such as termination
- an infrastructure architecture that fulfills these requirements, meets these risk tolerances, and implements effective controls (strong authentication, firewalls including ingress and egress filtering, enforcement of separation of duties, automated integrity checking, hot backups, etc.)
- review of all new and upgraded technologies that provide database support and in-house and remote access, to determine if any of these technologies introduce additional security risks or reduce existing risks. Review occurs before and after technology deployment.
- regular review and monitoring of relevant processes, and performance indicators and measures including financial performance and return on investment; regular review of new and emerging threats and evaluation of levels of risk
- regular audit of relevant controls and timely resolution of audit findings

Moulton and Coles offer another example of "how the information security governance concept could be applied at the enterprise level to establish and maintain an adequate control environment" [Moulton 03].

A level of adequate security as defined here is constantly changing in response to business and risk environments and the variation in risk tolerance that management is willing to accept. Effectively achieving and sustaining adequate security based on this definition is a continuous process, not a final outcome. Thus processes to plan for, monitor, review, report, and update an organization's security state must be part of normal day-to-day business conduct, risk management, and governance. This includes documenting this state and the best anticipation of its evolution as part of strategic and operational plans.

5 What Are the Characteristics of Effective Enterprise Security Governance?

In the preceding sections, we described some aspects and examples of how an organization can begin to think about governing to create and sustain a culture of security. In this section, we describe effective security governance in an organizational setting, including questions to ask, shifts in perspective, selection of foundational principles, and indicators of effectiveness.

All of these observations and recommendations are drawn from in-depth discussions and interviews, workshops, and work with leaders in organizations demonstrating an ability to achieve and sustain adequate security as defined in the previous section. In addition, confirmation of these beliefs, behaviors, capabilities, and actions is reflected in and synthesized from many of the references cited in this report.

5.1 Questions to Ask

Asking the following questions can help leaders determine the extent to which governance and enterprise-wide perspectives are being applied to security:[35]

- Do decision making and other key business processes take security concerns into account, such that the environment and the culture reflect due consideration of the value of assets, identified risks, and tolerable control of impacts and consequences?
- Does enterprise security have an appropriate level of representation and agenda visibility on the executive management committee? For board of directors' meetings?
- Do leaders (directors, senior executives, business-unit managers) understand the key enterprise security risks facing the organization?
- Have clear and separate accountabilities for enterprise-security governance and management activities been assigned?
- Have enterprise-security strategies been agreed to and are they understood by IT, security (CSO, CISO, or equivalent), and business-unit managers? Do business-unit managers understand their responsibility in the execution of these strategies?
- Conversely, does security management understand business strategies and priorities and reflect these in its decisions?
- Has the business agreed on objectives and performance metrics for enterprise security that include measurement and regular reporting of the value that it generates? Are

[35] This list of questions is derived in part from KPMG's information systems governance checklist for CEOs and boards [KPMG 04a].

awareness and education programs in place to ensure that the business gets the most value from enterprise security?

- Do the same project-governance principles and processes apply to both enterprise security and business projects, such as involving all the key stakeholders? Do project managers understand their responsibility for ensuring that business process changes for projects under their control do not violate the organization's information-security policies or compromise the security posture of the organization?
- Does enterprise security operate with the same risk-management processes as the rest of the business, and are formal processes employed—for example, is Audit involved when major changes are being made?
- Is the general auditor or chief audit executive regularly asking "What should we be doing to demonstrate sufficient control and oversight with respect to information security?"
- Is there evidence that all employees understand the organization's security policies and procedures as well as the reason they are in place and enforced?
- Is security considered a key operating principle that is reflected in the performance expectations of the business?

5.2 Shifts in Perspective

Security-conscious leaders ensure they are adequately and accurately informed with respect to risk management, business continuity, and organizational resilience, all of which affect security governance actions. In our research on managing for enterprise security, we discuss the necessity of a shift in perspective,[36] point of view, or frame of reference to be in a position to ask the right questions, as follows:

> Security lives in an organizational and operational context, not as an isolated discipline. Effective security must take into account the dynamically changing risk environment within which most organizations are expected to survive and thrive. To achieve and sustain an adequate level of security that directly supports the mission of the organization, leaders must shift their point of view (or frame of reference) and that of their organization from an information-technology-based, security-centric, technology-solution perspective to an enterprise-based, risk management, organizational continuity and resilience perspective. This requires moving well beyond ad-hoc, reactive approaches to security (lacking process and procedure, and dependent upon individual heroics) to approaches that are process centered, strategic, and adaptive. The CSO (and CISO) must be able to draw upon the capabilities of the entire organization so that they can be deployed to address a problem requiring an enterprise-wide solution set.

[36] Earlier work on shifts in perspective from security to survivability, including questions to ask to initiate each shift, can be found in the article "Information Survivability: Required Shifts in Perspective" [Allen 02].

However, because security isn't a one-shot activity, it also means being able to achieve it in a way that is sustainable—systematic, documented, repeatable, optimized, and adequate with respect to the organization's strategic drivers [Caralli 04c].

The presence of this shift in perspective increases the likelihood of involving the right stakeholders and obtaining the right information required to make well-informed governance decisions about security oversight, investment, and performance. The shifts most applicable to governance are briefly summarized below and in Table 1. They are covered in greater detail in our technical report *Managing for Enterprise Security* [Caralli 04c].

- **Scope**: Scope shifts from viewing security as a technical or technology-centric problem to viewing security as an enterprise-management problem. Scope answers the question, "What is the scope and extent of security concern within the enterprise?"
- **Ownership**: Ownership shifts from security being owned by those with technical expertise to security being owned by the business, which is the driver and ultimate benefactor. Ownership answers the questions "Who has the authority to act?" and "Who is accountable and responsible?"
- **Focus**: Focus shifts from an intermittent focus on security when something bad happens to security being treated as an accepted and expected business process and an included cost of doing business. Focus answers the question "How is security considered with respect to other fundamental enterprise operating principles?"
- **Funding**: Funding shifts from security being treated as a discretionary expense, burden, or tax to security being treated as an expense and investment for the business projects and processes it supports. Funding answers the questions "How does the organization fund the sustainment of adequate security?" and "How is security ROI calculated?"
- **Goal**: The goal shifts from leaders asking the question, "Are we secure?" to leaders asking the more useful and relevant question, "With respect to security, have we taken sufficient steps to ensure that the business and its critical assets are adequately protected and properly resilient?"

Table 1: Shifts in Perspective

Scope		
From: "Security is a technical problem."		**To**: "Security is an enterprise-wide problem."
• Technical network (hardware, software, infrastructure)		• Enterprise network (people, processes, business units)
• Technical requirements (protect the perimeter)	➡	• Enterprise requirements (privacy, asset protection)
• Technical assets (desktops, laptops, servers, databases)		• Enterprise assets (customer data, employee data, communication)
• Technical specialty (in the realm of IT and system administrators)		• Enterprise core competency

Ownership		
From: "Security has a technical owner." • IT is the driver, owner, and primary benefactor. • Technical personnel are responsible for security. • The CSO/CISO is considered a technical advisor.	➡	**To**: "Security is owned by the enterprise." • The enterprise is the driver, owner, and primary benefactor. • Business leaders understand security and have security responsibilities. • All employees understand their responsibilities with respect to security. • The CSO/CISO is considered an advisor to the business.
Focus		
From: "There is an intermittent focus on security." • Security is sporadically singled out for attention, investment, and justification. • Risk assessment is applied to security as a special case. • Security is on the agenda to comply with regulatory requirements.	➡	**To**: "Security is integrated." • Security is a requirement of conducting business, considered in normal planning and business-conduct cycles. • A more secure state results from effective risk-management capabilities. • Existing security controls meet compliance requirements.
Funding		
From: "Security is an expense." • The benefit of security is not measured or is hard to measure. • Return on security investments is not required or quantifiable.	➡	**To**: "Security is an investment." • The benefits of security are measurable, measured, and regularly reported. • Return on security investment is required and quantifiable in business terms. • Security expense and investment is part of all applicable business projects and processes.
Goal		
From: "The goal is security." • The focus of security efforts is on threat, vulnerability, and protection. • There is no articulated, desired security state.	➡	**To**: "The goal is business continuity and ultimately resiliency." • The focus of security efforts is on impact, organizational continuity, and preservation of trust.

• There is a potentially excessive deployment of security technologies undertaken in a piecemeal approach.		• Adequate security that meets business objectives is the desired state. • Security costs, benefits, and risks are in balance.

The next section describes foundational principles to consider when structuring an enterprise-security governance program.

5.3 Principle-Based Governance

Good governance derives from sound principles, often reflected in codes of conduct and practice. Sound principles apply to governing for enterprise security as well. *Enacted principles inform decisions thereby influencing policies, strategies, and plans. These actions create a culture of security throughout the enterprise.*

We have synthesized statements of information and enterprise security principles in the following topic areas:

- Accountability
- Adequacy
- Awareness
- Compliance
- Effectiveness
- Ethics
- Inclusion
- Individual Equity
- Information Sharing
- Measurement
- Perspective/Scope
- Response
- Risk Management

These topics and descriptions are derived from several credible and reputable organizations and the sources listed in Table 2.

Table 2: Sources of Enterprise-Security Principles

Organizations	References
American Chemistry Council	[ACC 99, ACC 03]
Business Software Alliance	[BSA 03]
Corporate Governance Task Force	[CGTF 04]
Corporate Information Security Working Group	[CISWG 04a, CISWG 04b]
Information Systems Security Association	[ISSA 04]
Information Technology Governance Institute	[ITGI 01, ITGI 04]
Institute of Internal Auditors	[IIA 01]
International Standards Organization (ISO)	[ISO 00a, ISO 00b]
National Association of Corporate Directors	[NACD 01]
National Institute of Standards and Technology	[NIST 96, NIST 04]
Organisation for Economic Co-operation and Development	[OECD 02]
Software Engineering Institute	[CMMI 03]

These principles represent a composite list; we expect that all principles are not applicable for all organizations. Organizations can use this list to select, interpret, prioritize, deploy, and reinforce statements of enterprise-security principles as manifestations of expected behaviors. To be effective and of greatest value, principle selections should be aligned with business objectives including the requirement to protect all stakeholder interests.

Principle descriptions in most of the references address the security of information. We expand these to address security of the extended enterprise that includes but is broader than information security.

Each of the principles is stated using the present tense, conveying what actions, behaviors, and conditions demonstrate the presence of the principle in the organization's culture and conduct.

- **Accountability**: The governing body (i.e., board of directors, trustees) is accountable for providing effective oversight of enterprise security. Management is responsible for ensuring effective execution of the agreed-to enterprise-security program. Such

accountability and responsibility is explicit, defined, acknowledged, and accompanied by the authority to act. Leadership accountability and responsibility for security are visible to all stakeholders (refer to Section 3.2 for a definition of "stakeholders").

Leaders (members of governing bodies and managers) possess the necessary knowledge, skills, and abilities to fulfill these responsibilities. Individual roles, responsibilities, authorities, and accountabilities are assigned. Leaders ensure that all stakeholders with access to enterprise networks understand their responsibilities with respect to enterprise security. Chief executives conduct regular enterprise-security evaluations, review the evaluation results with stakeholders as appropriate, and report on performance to the governing body, including a plan for remedial action to rectify any deficiencies.

- **Adequacy**: Investment in enterprise-security protection strategies (principles, policies, procedures, processes, controls) is commensurate with risk. Determination of risk is based on the value, sensitivity, and criticality of any asset with respect to its vulnerability to loss, damage, disclosure, or denied/interrupted access. Probability, frequency, and severity of potential vulnerabilities are considered along with a comparison of the cost to reconstitute the asset versus the cost to protect it (see Risk Management below). Dan Geer suggests that the most influential calibrator for the right amount of security investment is how much collaboration you have, meaning the amount of information you have "in play" resulting from how open your network is to outside parties [Geer 04b]. Other indicators may include the degree and circumstances of critical-asset exposure, or the range of tolerable to intolerable consequences resulting from a realized task.

  Leaders ensure that sufficient resources (people, time, equipment, facilities, dollars) are authorized and allocated to achieve and sustain an adequate level of security. Refer also to Section 5.

- **Awareness**: Leaders are aware of and understand the need to consider security from an enterprise-wide perspective, thus including it in their governance processes. They understand what actions are necessary to protect shareholder and stakeholder value with respect to security. They understand what enterprise-security actions are necessary to retain current customers and attract new customers.

  All stakeholders are aware of enterprise-security risks and protection strategies and understand their concomitant roles and responsibilities. Enterprise-security awareness is demonstrated by the motivation, training, and education provided to new stakeholders who become authorized users of enterprise networks and by attendance at periodic training as a requirement of continued access. Employee position descriptions defining security roles, responsibilities, skills, certifications, and agreements to comply with policy reflect awareness as well. Performance reviews include an evaluation of how well security responsibilities are fulfilled.

- **Compliance**: Enterprise-security protection strategies are in compliance with legal and regulatory requirements, requirements of conducting business, and requirements established by external stakeholders. Oversight and actions necessary to evaluate

compliance objectively (such as internal and external audits) are built into the enterprise-security program. This includes regular monitoring, review, and reporting of compliance findings to affected and interested parties.

Leaders ensure that a plan is developed to take remedial and timely action for any security deficiencies and ensure that the plan is effectively executed. "In many cases, getting and staying compliant all boils down to ensuring your corporation has well-documented and well-functioning processes" [Beauchamp 04].

- **Effectiveness**: Actions to achieve and sustain adequate enterprise security are demonstrably aligned with enterprise objectives, critical success factors, and the mitigation of enterprise-security risks. Security priorities and resources are determined based on this alignment. As a result, stakeholders view enterprise security in an enabling role, similar to audit, quality assurance, program management, and environmental protection [IIA 01]. Enterprise security is subject to continuous review, periodic testing, and an evaluation of its effectiveness as measured against enterprise objectives.
- **Ethics**: Use of information, systems, and networks across an enterprise and by all stakeholders matches expectations established by social norms, obligations, norms for responsible Internet citizenship, and enterprise codes of ethical conduct. Policies describing the ethical use of information address ownership, privacy, and prohibition of inappropriate use of information and systems to the detriment of an enterprise and its stakeholders. As a result, stakeholders are educated and thus respect the legitimate interests of others, understanding the extent to which their action or inaction may harm others and the consequences of unethical behavior.
- **Inclusion**: The perspective and requirements of all stakeholders are represented and considered in forming an enterprise-security strategy and program. This includes an appropriate level of stakeholder involvement in the development and review of principles, policies, procedures, processes, and controls. Inclusion is achieved through a range of communication and elicitation mechanisms such as Web sites, newsletters, regional meetings and conferences, and working groups.
- **Individual Equity**: Leaders implement enterprise security "in a manner consistent with the values of a democratic society including the freedom to exchange thoughts and ideas, the free flow of information, the confidentiality of information and communication, the appropriate protection of personal information, openness, and transparency" [OECD 02]. Enterprise security "actions do not infringe upon the obligations, rights and needs of legitimate users when exercised within the legitimate parameters of the mission objectives" [ISSA 04].
- **Information Sharing**: In response to the need for greater transparency and visibility, leaders are prepared to report the organization's security state to stakeholders when and where required, appropriately balanced with the risks of such disclosure. This includes ensuring that the right information is collected, retained, and communicated to the right parties at the right time. Forums for information sharing include those mentioned in Inclusion as well as interaction with oversight, regulatory, and law enforcement agencies.

- **Measurement**: Leaders articulate metrics whose measurement demonstrates the value and adequacy (or lack thereof) of enterprise security and the extent to which enterprise security actions are aligned with enterprise objectives (see Effectiveness). Such metrics indicate what leaders consider to be important. Peter Drucker states "What we measure and how we measure determine what will be considered relevant, and determine, thereby, not just what we see, but what we—and others—do" [Drucker 04].

  > What gets measured gets done. Metrics are about transforming policy into action and measuring performance. Visible metric scores provide a positive influence on human behavior by invoking the desire to succeed and compare favorably with one's peers. Metrics indicate how well policies and processes are functioning and whether or not they are producing desired performance outcomes [CISWG 04b].

  Metrics are defined and regularly reported at the governing-body, management, and technical levels of the enterprise. Performance measurement of an enterprise's security state is conducted with the same rigor as for other enterprise business units, functions, and processes.

- **Perspective/Scope**: The perspective, scope, and breadth of security is enterprise wide. "Security consciousness exists at all levels. Security is a holistic issue, including corporate culture, people, training, processes, and communications (not just technical concerns)" [IIA 01]. A coherent system of integrated security-protection strategies (principles, policies, procedures, processes, controls) exists to enact all of the principles described here and to ensure continuity of operations. "Security is a fundamental element of all products, services, systems, and networks" [OECD 02] and is considered at each phase of any development and asset life cycle. Staff and stakeholders understand that security is an essential business requirement and thus a characteristic or attribute of how the organization conducts itself.
- **Response**: All accountable stakeholders act in a timely, coordinated manner to prevent or respond to threats to enterprise security and compromises of enterprise security. Such response requires development and regular exercise of business-continuity, disaster-recovery, crisis-management, and incident-management plans so that the enterprise is adequately prepared in the face of an attack and is able to resume normal operations as quickly as possible.
- **Risk Management**: Leaders continually review, assess, and modify enterprise-security protection strategies in response to the dynamically changing risk environment in which they operate. This includes "potential harm that may originate from others or be caused by others" [OECD 02]. Leaders articulate acceptable levels of risk (tolerance, appetite, thresholds, assumptions for same) to enterprise assets based on their value, sensitivity, and criticality (see Adequacy). Such levels are examined during regular review and assessment processes.

  Costs of compromise (loss, damage, disclosure, denied/interrupted access, costs to reconstitute) are quantified to the extent possible as part of ongoing risk management. Controls are selected to effectively mitigate risk and their performance is regularly

measured and reviewed. Plans for remedial action to rectify risk-mitigation deficiencies are developed and executed following each assessment.

5.4 Indicators of Effectiveness

The following beliefs, behaviors, capabilities, and actions indicate the presence of a culture of security, thus demonstrating a governance perspective with respect to security as described in this report.

- Security is addressed and enacted at an enterprise level. Leaders understand their accountability and responsibility with respect to security for the organization, for their stakeholders, and for the communities they serve, including the Internet community and the protection of critical national infrastructures.
- Security is an expected topic of discussion among decision makers when business issues arise and is given the same level of respect as other fundamental drivers and influencing elements of the business.
- With respect to oversight, planning, and performance, security is treated in the same fashion as any other business requirement. Security is considered a cost of doing business, not a discretionary or negotiable budget-line item that needs to be regularly defended. Business units and staff don't get to decide unilaterally how much security they want. Adequate and sustained funding and allocation of security resources are required as part of the operational projects and processes they support.
- Security appears regularly as a topic on executive management and boards of directors' meeting agendas, both separately and as it affects and relates to other topics.
- Security is addressed during normal strategic and operational planning cycles. Security has achievable, measurable objectives that directly align with enterprise objectives. Determining how much security is enough equates to how much risk and exposure an organization can tolerate.
- Communication, discussion, and debate on security topics are encouraged. Such exchanges are conducted in visible, open, participative forums, both formal and informal, as appropriate. Security actions and their contribution to mitigation of enterprise risk are known throughout the organization.
- An organization regularly compares and benchmarks its security state, investments, and actions with others in its market sector and community of practice.
- Security leaders are well respected in the enterprise culture, are perceived as valued contributors whose opinions and expertise are sought, navigate freely across the organization, regularly collaborate with peers (including the general auditor, treasurer/CFO, and corporate legal), and have a seat at the table for major business initiatives.

- All functions and business unit leaders within the organization understand how security serves as a business enabler (versus an inhibitor). They understand that their performance with respect to security is measured as part of their overall performance.
- Security is integrated into enterprise functions and processes. These include risk management, human resources (hiring, firing), audit/compliance, disaster recovery, business continuity, asset management, change control, and IT operations. Security is actively considered as part of new project initiation and ongoing project management and during all phases of any system-development life cycle (applications and operations).
- While the security function has a close working relationship and interdependency with IT, security is not viewed solely as an IT responsibility.
- All personnel who have access to enterprise networks understand their individual responsibilities for protecting and preserving the organization's security condition. Rewards, recognition, and consequences for security-policy compliance are consistently applied and reinforced.

Leaders can use the questions posed in Section 5.1 to determine to what extent their organizations consider security from both governance and enterprise-wide perspectives, and if this makes sense based on enterprise mission and objectives.

Leaders committed to establishing and sustaining a culture of security in their organizations can examine their own mental models using the shifts in perspectives described in Section 5.2, and the degree to which these shifts have occurred. They can then select principles (defined in Section 5.3) that effectively support the accomplishment of business objectives through the deployment of protection strategies including policies, procedures, processes, controls, allocation of resources, and measurement. Indicators of effectiveness (described in Section 5.4) can be used to help determine progress along the path when played against the organization's working definition of adequate security (discussed in Section 4).

6 Future Work

As stated in the introduction, our desired outcomes for this report are to increase awareness, understanding, and education, and to encourage action to address security at an enterprise level and as a governance concern. Our work in determining the extent to which security needs to be a governance concern is an applied-research work in progress that benefits from broader communication, feedback, and community involvement. To realize these outcomes and benefits, we hope that readers of this report will contact us to

- share this report with their constituencies
- identify organizations and sources working in this research area beyond those cited that can provide additional value, divergent perspectives, and experience reports
- express interest in participating as a collaboration, benchmark, and/or case-study partner

Assuming these outcomes are realized in whole or in part, our intent is to continue this work in the following directions:[37]

- Work with collaboration, benchmark, and case-study partners to identify specific implementations of effective programs where security is being addressed from both enterprise and governance perspectives; capture key principles, policies, procedures, processes, practices, and measures; document these with attribution where appropriate, deriving and recommending strategies that will help organizations develop their own approaches for enterprise-security governance.
- Communicate this work in venues of interest including selected conferences and in publications.
- Build a community of practice that is interested in moving this work forward and contributing to its maturation and transition.

[37] Please contact the author at jha@sei.cmu.edu or jha@cert.org if you have an interest in this work.

Appendix A Sources for Governance and Enterprise-Based Security Principles, Guidelines, and Practices

This appendix provides examples from several market sectors and organizations describing how they have successfully addressed security at both enterprise and governance levels based on guiding principles. Several of these examples provide sufficient detail for implementing such a program.

American Chemistry Council

The American Chemistry Council states the following on its Web site:[38]

> The American Chemistry Council represents the leading companies engaged in the business of chemistry. Council members apply the science of chemistry to make innovative products and services that make people's lives better, healthier and safer. The Council is committed to improved environmental, health and safety performance through Responsible Care, common sense advocacy designed to address major public policy issues, and health and environmental research and product testing.

The ACC's Responsible Care®[39] program is an excellent example of governance in action for a market sector. This program

- resulted in reduced emissions of 70 percent
- has an employee safety record that is four times better than the average of the U.S. manufacturing sector
- helps America's leading chemical companies go above and beyond government requirements and openly communicate their results to the public
- results in companies improving their performance by implementing world-class management practices, extending these best practices to business partners throughout the industry

Through the Responsible Care® Metrics Web site[40], these companies are making available the most performance information of any private sector industry group, a demonstration of the information sharing principle described in Section 6.3.

[38] http://www.americanchemistry.com

[39] Responsible Care is a registered service mark of the American Chemistry Council.

The ACC's Responsible Care program includes a security code of 13 management practices with stated principles. Implementation of this security code is mandatory for all ACC members. Additional guidance is available in their *Implementation Guide for Responsible Care Security Code of Management Practices* [ACC 02].

Here are some excerpts from the code:

> The purpose of the Security Code is to help protect people, property, products, processes, information and information systems by enhancing security, including security against potential terrorist attack, throughout the chemical industry value chain. The chemical industry value chain encompasses company activities associated with the design, procurement, manufacturing, marketing, distribution, transportation, customer support, use, recycle and disposal of our products.
>
> This Code is designed to help companies achieve continuous improvement in security performance using a risk-based approach to identify, assess and address vulnerabilities, prevent or mitigate incidents, enhance training and response capabilities, and maintain and improve relationships with key stakeholders. The Code must be implemented with the understanding that security is a shared responsibility requiring actions by others such as customers, suppliers, service providers, and government officials and agencies. Everyone in the chemical industry value chain has security responsibilities and must act accordingly to protect the public interest.

Principles called out in the Security Code are as follows:

- To operate our facilities in a manner that protects the environment and the health and safety of our employees and the public.
- To lead in the development of responsible laws, regulations and standards that safeguard the community, workplace and environment.
- To work with customers, carriers, suppliers, distributors and contractors to foster the safe use, transport, and disposal of chemicals.
- To seek and incorporate public input regarding our products and operations.
- To make health, safety, the environment and resource conservation critical considerations for all new and existing products and processes.
- To practice Responsible Care by encouraging and assisting others to adhere to these principles and practices.

[40] http://www.responsiblecare-us.com

The ACC is a member of the Chemical Sector Cybersecurity Program, which states the following on its Web site:[41]

> Cybersecurity is integral to our overall national security, especially as our sector becomes increasingly dependent on inter-company connectivity. Stemming from the sector's long history of proactively addressing issues of global importance, the Chemical Sector Cybersecurity Information Sharing Forum was created in April 2002 to implement a cybersecurity program focused on risk management and reduction. The Forum consists of senior-level officials and/or staff representatives of 10 trade associations representing more than 2,000 companies from key industry segments within the sector. Its focus is on promoting the use of open, secure information and process control systems to help protect communities and facilitate business operations.
>
> The Forum appointed a taskforce of experts from a variety of disciplines to execute its first order of business, the development of an industry-wide cybersecurity strategy. The U.S. Chemical Sector Cybersecurity Strategy was fully endorsed by the industry in June 2002, delivered to the U.S. government in July 2002 and is referenced in the February 2003 release of the National Strategy to Secure Cyberspace.
>
> The Strategy defines a risk-based program designed to help protect information and keep operations safe. As a part of the Program, the Forum is responsible for fostering involvement and commitment among sector companies, coordinating sector positions on cybersecurity public affairs issues and driving the adoption of Program recommendations throughout the sector.

Corporate Governance Task Force

The Corporate Governance Task Force was chartered as a result of a December 2004 National Cyber Security Summit. The summit was hosted by the U.S. Department of Homeland Security with leading industry associations, including the U.S. Chamber of Commerce, the Business Software Alliance, the Information Technology Association of America, and TechNet.

The task force produced its final report titled "Information Security Governance: A Call to Action" [CGTF 04]. The report defines a core set of principles and makes four recommendations, included below. The report also provides a comprehensive information-security governance framework, functions and responsibilities guides, and assessment approaches.

Core Principles

- CEOs should conduct an annual information security evaluation, review the evaluation results with staff, and report on performance to the Board of Directors.

[41] http://www.chemicalcybersecurity.com/forum/

- Organizations should conduct periodic risk assessments of information assets as part of a risk management program.
- Organizations should implement policies and procedures based on risk assessments to secure information assets.
- Organizations should establish a security management structure to assign explicit individual roles, responsibilities, authority, and accountability.
- Organizations should develop plans and initiate actions to provide adequate information security for networks, facilities, systems and information.
- Organizations should treat information security as an integral part of the system life cycle.
- Organizations should provide information security awareness, training, and education to personnel.
- Organizations should conduct periodic testing and evaluation of the effectiveness of information security policies and procedures.
- Organizations should create and execute a plan for remedial action to address any information security deficiencies.
- Organizations should develop and implement incident response procedures.
- Organizations should establish plans, procedures, and tests to provide continuity of operations.
- Organizations should use security best practices guidance, such as ISO 17799, to measure information security performance.

Recommendations

Recommendation 1: Organizations should adopt the information security governance framework described in this report to embed cyber security into their corporate governance process.

Recommendation 2: Organizations should signal their commitment to information security governance by stating on their Web site that they intend to use the tools developed by the Corporate Governance Task Force to assess their performance and report the results to their board of directors.

Recommendation 3: All organizations represented on the Corporate Governance Task Force should signal their commitment to information security governance by voluntarily posting a statement on their Web site. In addition, TechNet, the Business Software Alliance, the Information Technology Association of America, the Chamber of Commerce, and other leading trade associations and membership organizations should encourage their members to embrace information security governance and post statements on their Web sites. Furthermore, all Summit participants should embrace information security governance and post statements on their Web sites, and if applicable, encourage their members to do so as well.

Recommendation 4: The Department of Homeland Security should endorse the information security governance framework and core set of principles outlined in this report, and encourage the private sector to make cyber security part of its corporate governance efforts.

The work of the CGTF is additionally described in the article "A Framework for the Governance of Information Security" [Posthumus 04].

Corporate Information Security Working Group

The Corporate Information Security Working Group (CISWG) was convened by Representative Adam Putnam (R-FL) and met from November 2003 through November 2004. The CISWG Phase II Best Practices and Metrics Team had as its goal to "develop a resource that would help Board members, managers, and technical staff establish their own comprehensive structure of principles, policies, processes, controls, and performance metrics to support the people, process, and technology aspects of information security" [CISWG 04b]. This team's Phase II report [CISWG 04b] gives detailed descriptions of the Information Security Program Elements (ISPE) for Governance and Management outlined below:

A. Governance (Board of Directors/Trustees)

1. Oversee Risk Management and Compliance Programs Pertaining to Information Security (e.g., Sarbanes-Oxley, HIPAA, Gramm-Leach-Bliley) (ISPE1)
2. Approve and Adopt Broad Information Security Program Principles and Approve Assignment of Key Managers Responsible for Information Security (ISPE2)
3. Strive to Protect the Interests of all Stakeholders Dependent on Information Security (ISPE3)
4. Review Information Security Policies Regarding Strategic Partners and Other Third-Parties (ISPE4)
5. Strive to Ensure Business Continuity (ISPE5)
6. Review Provisions for Internal and External Audits of the Information Security Program (ISPE6)
7. Collaborate with Management to Specify the Information Security Metrics to be Reported to the Board (ISPE7)

B. Management

8. Establish Information Security Management Policies and Controls and Monitor Compliance (ISPE8)
9. Assign Information Security Roles, Responsibilities, Required Skills, and Enforce Role-based Information Access Privileges (ISPE9)
10. Assess Information Risks, Establish Risk Thresholds and Actively Manage Risk Mitigation (ISPE10)

11. Ensure Implementation of Information Security Requirements for Strategic Partners and Other Third-parties (ISPE11)
12. Identify and Classify Information Assets (ISPE12)
13. Implement and Test Business Continuity Plans (ISPE13)
14. Approve Information Systems Architecture during Acquisition, Development, Operations, and Maintenance (ISPE14)
15. Protect the Physical Environment (ISPE15)
16. Ensure Internal and External Audits of the Information Security Program with Timely Follow-up (ISPE16)
17. Collaborate with Security Staff to Specify the Information Security Metrics to be Reported to Management (ISPE17)

CSO Magazine

CSO Magazine has published a series of articles[42] that address the topic of security convergence, also known as holistic or integrated security, describing the need for an enterprise-wide approach for security. They raise the following question [Slater 05]:

> Why not bring security-focused departments together proactively, aggregating their information and expertise to look at operational risk as a unified picture and create a security plan that is more effective, more cost-efficient, and more credible to upper management?

Slater defines convergence as "Integrating historically stovepiped functions of operational risk management to achieve better security, oversight of enterprise wide risk, and cost efficiencies." The article "Security 2.0" provides a convergence case study for Constellation Energy.

CSO also published a useful example of what can happen when an effective security governance program is absent, in their article titled "The Five Most Shocking Things About the ChoicePoint Debacle" [Scalet 05].

Federal Financial Institutions Examination Council

The Federal Financial Institutions Examination Council states the following on its Web site[43]:

> The Council is a formal interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions by the Board of Governors of the Federal Reserve System (FRB), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union

---

[42] http://www.csoonline.com/read/041505/intro.html

[43] http://www.ffiec.gov

Administration (NCUA), the Office of the Comptroller of the Currency (OCC), and the Office of Thrift Supervision (OTS) and to make recommendations to promote uniformity in the supervision of financial institutions.

The FFIEC IT Examination handbook series volumes on management [FFIEC 02] and information security [FFIEC 04] state the following:

> The board of directors is responsible for overseeing the development, implementation, and maintenance of the institution's information security program. Oversight requires the board to provide management with guidance and receive reports on the effectiveness of management's response. The board should approve written information security policies and the information security program at least annually. The board also should provide management with its expectations and requirements for:
>
> 1. Central oversight and coordination
> 2. Areas of responsibility
> 3. Risk measurement
> 4. Monitoring and testing
> 5. Reporting
> 6. Acceptable residual risk

These handbooks serve as excellent resources for an enterprise security governance program.

ISO 17799

The International Standards Organisation ISO/IEC 17799 *Information Technology Code of Practices for Information Security Management* [ISO 00b] is often cited as one of the most authoritative sources for defining and deploying an enterprise-wide approach to information security. ISO 17799 states the following:

> Critical success factors: Experience has shown that the following factors are often critical to the successful implementation of IS within an organization:
>
> - Security policy, objectives, and activities that reflect business objectives
> - An approach to implementing security that is consistent with the organizational culture
> - Visible support and commitment from management
> - A good understanding of the security requirements, risk assessment, and risk management
> - Effective marketing of security all managers and employees
> - Distribution of guidance on IS policy and standards to all employees and contractors
> - Providing appropriate training and education

- A comprehensive and balanced system of measurement which is used to evaluate performance in IS mgmt and feedback suggestions for improvement

National Association of Corporate Directors

The National Association of Corporate Directors defines the following essential practices in its guide titled "Information Security Oversight: Essential Board Practices" [NACD 01]:

- Essential Practice 1: Place information security on the board's agenda
- Essential Practice 2: Identify information security leaders; hold them accountable, and ensure support for them
- Essential Practice 3: Ensure the effectiveness of the corporation's information security policy through review and approval
- Essential Practice 4: Assign information security to a key committee

More broadly, the NACD convened a Blue Ribbon Commission on Risk Oversight, co-chaired by Norman Augustine and Ira Millstein. The January 2003 *Director's Monthly* newsletter [NACD 03] provides excerpts from this report that describe

- The challenges of oversight
- Five major issues for boards
- Meeting the challenge of turbulent times through risk oversight
- Building a foundation of good corporate governance
- Overseeing risk management
- Addressing specific risks and preparing for crisis
- Responding to and learning from crisis
- Benefits of risk oversight

Given that security is a risk-management issue, all of these points are relevant to governing for enterprise security.

The SEI Networked Systems Survivability Program: Enterprise Security Management

In an outgrowth of on-site work deploying information-security risk-assessment methodologies, a team in the Networked Systems Survivability program at the Software Engineering Institute (SEI) is identifying and examining the core capabilities that define a framework for security management in an organizational and operational context. In this context, the practice of security is viewed as an activity that keeps the organization's productive elements—people, assets, and technology—free from harm or disruption so that they can perform their intended functions and help the organization accomplish its mission. ESM and the work described in this report are complementary, with governing for enterprise security providing the oversight, decision making, and accountability framework and ESM providing the management and implementation framework.

ESM work in progress includes development of a capabilities framework that represents the essential capabilities necessary for treating security as a business problem. This framework is intended to document and describe the core capabilities necessary for a systematic, managed, and measured process for securing the assets and processes of medium to large organizations. (Further information is available in several reports by Rich Caralli [Caralli 04a, Caralli 04b, Caralli 04c, Caralli 05].)

Visa's Cardholder Information Security Program

Visa's Cardholder Information Security Program (CISP) is an example of security governance extended to all merchants as a condition of their use of Visa services for their customers.

Visa's CISP Web site states the following:[44]

> When customers offer their bankcard at the point of sale, over the Internet, on the phone, or through the mail, they want assurance that their account information is safe. That's why Visa USA has instituted the Cardholder Information Security Program (CISP). Mandated since June 2001, the program is intended to protect Visa cardholder data—wherever it resides—ensuring that members, merchants, and service providers maintain the highest information security standard.
>
> CISP compliance is required of all merchants and service providers that store, process, or transmit Visa cardholder data. The program applies to all payment channels, including retail (brick-and-mortar), mail/telephone order, and e-commerce. To achieve compliance with CISP, merchants and service providers must adhere to the Payment Card Industry (PCI) Data Security Standard, which offers a single approach to safeguarding sensitive data for all card brands. This Standard is a result of a collaboration between Visa and MasterCard and is designed to create common industry security requirements, incorporating the CISP requirements. Other card companies operating in the U.S. have also endorsed the PCI Data Security Standard within their respective programs.

The PCI Data Security Standard is publicly available and consists of 12 basic requirements in the following categories:

Build and maintain a secure network

1. Install and maintain a firewall configuration to protect data
2. Do not use vendor-supplied defaults for system passwords and other security parameters

Protect cardholder data

3. Protect stored data

[44] http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp.html

4. Encrypt transmission of cardholder data and sensitive information across public networks

Maintain a vulnerability management program

5. Use and regularly update anti-virus software
6. Develop and maintain secure systems and applications

Implement strong access control measures

7. Restrict access to data by business need-to-know
8. Assign a unique ID to each person with computer access
9. Restrict physical access to cardholder data

Regularly monitor and test networks

10. Track and monitor all access to network resources and cardholder data
11. Regularly test security systems and processes

Maintain an information security policy

12. Maintain a policy that addresses information security

This standard is also included and expanded upon as part of MasterCard's Site Data Protection Program.[45] Additional standards described at the MasterCard site include PCI Security Scanning Procedures, PCI Security Audit Procedures, and a PCI Self-Assessment Questionnaire.

[45] https://sdp.mastercardintl.com/

Appendix B Governance Definitions

Corporate Governance

The Organization for Economic Development (OECD) defines "corporate governance" as follows:

> Corporate governance involves a set of relationships between a company's management, its board, its shareholders, and other stakeholders. Corporate governance also provides the structure through which the objectives of the company are set, and the means of attaining those objectives and monitoring performance are determined. Good corporate governance should provide proper incentives for the board and management to pursue objectives that are in the interests of the company and its shareholders and should facilitate effective monitoring [OECD 04].

Definitions of corporate governance are sometimes constrained to address financial reporting; the accountability of boards of directors (or equivalent), CEOs, and other senior executives; and responsibilities to shareholders.

The recently published Corporate Governance Task Force Report *Information Security Governance: A Call for Action* [CGTF 04] defines corporate governance as "the set of policies and internal controls by which organizations, irrespective of size or form, are directed and managed."

Governance regulates "the rights and obligations of all parties involved." It is a contract between people and provides a roadmap defining mutual and individual roles and responsibilities. It is about culture, ethics, and adapting to internal and external circumstances and influences [KPMG].

Enterprise Governance

The Information Systems and Control Audit Association (ISACA) and the Information Technology Governance Institute (ITGI) define "enterprise governance" as follows. There is some overlap between this definition and those for corporate governance:

> The set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the enterprise's resources are used responsibly [ITGI 03].

This definition has also been adopted by The Chartered Institute of Management Accountants (CIMA) [CIMA 04] and the International Federation of Accountants [IFAC 04].

IT Governance

Gartner states that

> IT governance specifies the decision-making authority and accountability to encourage desirable behaviors in the use of IT. IT governance provides a framework in which the decisions made about IT issues are aligned with the overall business strategy and culture of the enterprise. Governance is about decision making per se—not about how the actions resulting from the decisions are executed. Governance is concerned with setting directions, establishing standards and principles, and prioritizing investments; management is concerned with execution [Dallas 04].

ITGI defines IT governance as "the leadership, organizational structures, and processes that ensure that the enterprise's IT sustains and extends the enterprise's strategies and objectives." ITGI also states that "While governance developments have primarily been driven by the need for the transparency of enterprise risks and the protection of shareholder value, the pervasive use of technology has created a critical dependency on IT that calls for a specific focus on IT governance" [ITGI 03]. Considering both of these definitions, much the same can be said for enterprise security and, in fact, ITGI has created a companion report on Information Security Governance [ITGI 01].

The report "Creating Stakeholder Value in the Information Age: The Case for Information Systems Governance" [KPMG] states that information systems (IS) governance is

- an integral part of corporate governance
- the responsibility of board members and executives
- a mechanism to deliver value, manage performance, and mitigate risk
- a method to assign accountability for decisions and performance
- dynamic in alignment to business goals
- composed of policies, procedures, management committees, performance metrics, and related management techniques working in unison toward common business goals

IS governance is the set of rules and agreements intended to govern decision-making regarding the information supply within the organization [KPMG].

According to Peter Weill and Jeanne Ross [Weill 04], IT governance consists of "specifying the decision rights and accountability framework to encourage desirable behavior in the use of IT. Governance determines who makes the decisions. Management is the process of making and implementing the decisions. IT governance is the most important factor in generating business value from IT."

According to Weill and Ross, effective IT governance must answer three questions:

1. What decisions must be made to ensure effective management and use of IT?
2. Who should make these decisions?
3. How will these decisions be made and monitored?"

Regarding IT governance, Willie Appel states that "IT governance is about assigning decisions rights and creating an accountability framework that encourages desirable behavior in the uses of information and technology. It is the principles, people, processes, and performance metrics that enable and provide the means to ensure freedom of actions/decisions across the enterprise without suboptimizing the enterprise" [Appel 04].

Information Security Governance

Moulton defines information security governance as "the establishment and maintenance of the control environment to manage the risks relating to the confidentiality, integrity, and availability of information and its supporting processes and systems" [Moulton 03]. This is separate from

- audit (ensuring that governance processes have been properly established and are functioning)
- security operations (day-to-day performance of security administrative activities)
- security development (engineering of new IT or processes to meet security objectives)

Appendix C C-Level Target Audience

The C-level audience we hope to reach either directly or through the CIO, CSO, and CISO are those with responsibilities to define and deploy governance-level actions. These may include:

- CEO (Chief Executive Officer), President
- CAE (Chief Audit Executive), General Auditor, and Directors of IT Audit
- CCO (Chief Compliance Officer), growing in response to the U.S. Sarbanes-Oxley Act
- Chief Ethics Officer
- CFO (Chief Financial Officer)
- CGO (Chief Governance Officer), emerging in response to the growth of organizational activities now labeled as matters for board oversight as well as management activity (for example, the audit committees of New York Stock Exchange-listed companies must include legal compliance oversight as part of their charter)
- CKO (Chief Knowledge Officer)
- Chief Legal Officer; General Counsel
- CPO (Chief Privacy Officer)
- CRO (Chief Risk Officer)

Bibliography

URLs are valid as of the publication date of this document.

[Allen 04, 05a] Allen, Julia. Articles in the Governing for Enterprise Security series:

- "Governing for Enterprise Security: An Introduction" (June 2004)
- "Be Aware and Understand" (July 2004)
- "Shifts in Perspective" (August 2004)
- "Protect Stakeholder Interests" (October 2004)
- "How Much Security Is Enough?" (January 2005)

http://www.cert.org/nav/index_green.html

[Allen 05b] Allen, Julia. "How Do I Know If I Have a Culture of Security?" *Enterprise Risk Management & Governance E-Mail Advisor*, Cutter Consortium, April 2005.

[Berinato 04] Berinato, Scott. "Locked Out." *CSO Magazine*, July 2004. http://www.csoonline.com/read/070104/cisco.html.

[Brechbuhl 05] Brechbuhl, Hans & Dynes, Scott. "Driving Change in Corporate Information Security: Tuck School of Business." CIO.com, June 2005. http://www2.cio.com/higher/report3660.html (2005).

[BRT 03] Business Roundtable. *Building Security in the Digital Economy.* http://www.businessroundtable.org/publications /publication.aspx?qs=27B6BF807822B0F19D640 (2003).

[BSI 02] British Standards Institute. *Information security management systems–Specification with guidance for use*. BS7799-2:2002, September 2002.

[Campbell 03] Campbell, Katherine; Gordon, Lawrence; Loeb, Martin; Zhou, Lei. "The economic cost of publicly announced information security breaches; empirical evidence from the stock market." *Journal of Computer Security 11*, 3 (March 2003).

[Chapin 05] Chapin, David & Akridge, Steven. "How Can Security Be Measured?" *Information Systems Control Journal, 2*. Information Systems Audit and Control Association, 2005.

[CICA 04] The Canadian Institute of Chartered Accountants. "20 Questions Directors Should Ask About IT." CICA, April 2004. http://www.cica.ca/index.cfm/ci_id/1000/la_id/1.htm.

[CIDX 04] Chemical Industry Data Exchange. *Guidance for Addressing Cybersecurity in the Chemical Sector*, Version 2.0, CIDX, 2004. http://www.cidx.org/CyberSecurity/publications/default.asp.

[CIO 04] CIO Research Reports. "State of the CSO 2004." CIO.com, June 1, 2004. http://www2.cio.com/research/surveyreport.cfm?id=72.

[CSTB 02] Computer Science and Telecommunications Board. *Cybersecurity Today and Tomorrow: Pay Now or Pay Later*, National Academy Press, Washington, D.C., 2002. http://www7.nationalacademies.org/cstb/pub_cybersecurity.html.

[Cramm 03] Cramm, Susan. "A Cry for Full-Cycle Governance." CIO.com, Aug 1, 2003. http://www.cio.com/archive/080103/hs_agenda.html.

[CRS 04a] Cashell, Brian, et al. "The Economic Impact of Cyber-Attacks." Order Code RL32331. Congressional Research Service, Library of Congress, April 1, 2004. http://www.cisco.com/warp/public/779 /govtaffairs/images/CRS_Cyber_Attacks.pdf

[CRS 04b] Moteff, John. "Computer Security: A Summary of Selected Federal Laws, Executive Orders, and Presidential Directives." Order Code RL32357. Congressional Research Service, Library of Congress, April 16, 2004. http://www.fas.org/irp/crs/RL32357.pdf.

[Dodds 04] Dodds, Rupert. "Effective Information Technology Governance Will Improve Returns to Shareholders." *Information Systems Control Journal, 3*. ISACA, 2004.

[Ernst 04] Ernst & Young. "Global Information Security Survey 2004." http://www.ey.com/global/download.nsf/UK /Survey_-_Global_Information_Security_04/$file /EY_GISS_%202004_EYG.pdf.

[Friedman 05] Friedman, Thomas. *The World Is Flat: A Brief History of the Twenty-first Century*, Farrar, Straus and Giroux, 2005.

[Friedman 00] Friedman, Thomas. *The Lexus and the Olive Tree: Understanding Globalization*, Anchor Books, 2000.

[Hamaker 03a] Hamaker, Stacey. "Spotlight on Governance." *Information Systems Control Journal, 1.* ISACA, 2003.

[Hamaker 03b] Hamaker, Stacey & Hutton, Austin. "Principles of Governance." *Information Systems Control Journal, 3.* ISACA, 2003.

[Hamaker 04] Hamaker, Stacey & Hutton, Austin. "Principles of IT Governance." *Information Systems Control Journal, 2.* ISACA, 2004.

[Hamel 04] Hamel, Gary & Valikangas, Liisa. "The Quest for Resilience," *Harvard Business Review*, September 2003.

[IIA 00] The Institute of Internal Auditors et al. "Information Security Management and Assurance: A Call to Action for Corporate Governance." IIA, April 2000. http://www.theiia.org/iia/index.cfm?doc_id=3061.

[IIA 04] The Institute of Internal Auditors. "Applying COSO's Enterprise Risk Management Framework." IIA, September 2004. http://www.theiia.org/iia/download.cfm?file=7751.

[IIA 05a] The Institute of Internal Auditors. "Global Technology Audit Guides: Information Technology Controls." IIA, March, 2005. http://www.theiia.org/index.cfm?doc_id=4706.

[ISF 04] Information Security Forum. "Information Risk Management in Corporate Governance: Overview Report." ISF, 2004.

[JF 05] Jericho Forum. "Visioning White Paper (on de-perimeterisation)." Jericho Forum, February 2005. http://www.opengroup.org /projects/jericho/uploads/40/6809/vision_wp.pdf.

[LeGrand 03a] Le Grand, Charles. "Audit & Security Controls That Work: Information Security Governance and Assurance." Slides presented at SANS Audit & Security Controls That Work Technical Conference. The Institute of Internal Auditors, April 5, 2003.

[LeGrand 03b] Le Grand, Charles. "Information Security Governance and Assurance." White paper presented at SANS Audit & Security Controls That Work Technical Conference, SANS Institute, 2003.

[Levinson 04] Levinson, Meredith. "Who's Afraid of the Big, Bad Board?" *CIO Magazine*, September 2004. http://www.cio.com /archive/091504/board.html.

[McFadzean 03] McFadzean, Elspeth; Ezingeard, Jean-Noel; & Birchall, David. Boards of Directors' Engagement with Information Security; HWP 0309" Henley Management College Working Paper Series, Henley Management College, 2003.

[McFadzean 04] McFadzean, Elspeth; Ezingeard, Jean-Noel; & Birchall, David. "Anchoring Information Security Governance Research: Sociological Groundings and Future Directions." Henley Management College, Third Security Conference, eds. Dhillon, G. & Furnell, S., Las Vegas, Nevada, USA, 2004.

[Milus 04] Milus, Stu. "The Institutional Need for Comprehensive Auditing Strategies." *Information Systems Control Journal, 6.* Information Systems Audit and Control Association, 2004.

[Moxey 04] Moxey, Paul. "Corporate Governance and Wealth Creation: Occasional Research Paper No. 37." The Association of Chartered Certified Accountants, 2004. http://www.accaglobal.com /research/summaries/2281270.

[Murray 04] Murray, Sarah. "Boards consider the value of protection." *Financial Times*, April 2004. http://news.ft.com/servlet /ContentServer?pagename=FT.com/StoryFT/FullStory&c=StoryFT& cid=1079420344085&p=1059479525589.

[NIST 03] National Institute of Standards and Technology. "Standards for Security Categorization of Federal Information and Information Systems; FIPS PUB 199. Federal Information Processing Standards Publication, NIST, December 2003. http://csrc.nist.gov/publications/fips/.

[NIST 05] Ross, Ron, et al. "Recommended Security Controls for Federal Information Systems" (NIST Special Publication 800-53). National Institute of Standards and Technology. http://csrc.nist.gov /publications/nistpubs/800-53/SP800-53.pdf. (February 2005.)

[OCEG 04] Open Compliance and Ethics Group. "Foundation Guidelines Red Book: Public Exposure Draft." OCEG, May 2004. http://www.oceg.org/exposureDraft.asp.

[Ross 04] Ross, Jeanne & Weill, Peter. "Recipe for Good Governance." *CIO Magazine*, June 15, 2004. http://www.cio.com/archive/061504 /keynote.html.

[Royds 05] Royds, James. "A Corporate Information Governance Agenda: Integrating Business Continuity and Security Management." *Enterprise Risk Management and Governance Advisory Service Executive Report, 2*, 4. Cutter Consortium, 2005.

[Schneier 04] Schneier, Bruce. "Hacking the Business Climate for Network Security." *Computer*, IEEE, April 2004.

[Sherman 04] Sherman, Erik. "Prove It: Get Your Security Act Together or Adam Putnam Will Do It for You." *Information Security Magazine*, May 2004. http://infosecuritymag.techtarget.com/ss /0,295796,sid6_iss386_art743,00.html.

[Sherwood 03] Sherwood, John; Clark, Andrew; & Lynas, David. "Systems and Business Security Architecture." SABSA Limited, 17 September 2003. http://www.alctraining.com.au/pdf/SABSA_White_Paper.pdf.

[Starr 03] Starr, Randy; Newfrock, Jim; & Delurey, Michael. "Enterprise Resilience: Managing Risk in the Networked Economy." strategy+business, Spring 2003.[46]

[Van Decker 04] Van Decker, John & Lepeak, Stan. "Building a Corporate Governance Framework That Leverages IT's Contribution." META Group, March 10, 2004. http://www.metagroup.com/us/displayArticle.do?oid=47695.[47]

[Van Grembergen 04] Van Grembergen, Wim. *Strategies for Information Technology Governance*, Chapter VI, Idea Group Publishing, 2004.[48]

[Zoellick 05] Zoellick, Bill & Frank, Ted. "Governance, Risk Management, and Compliance: An Operational Approach." Public Draft Version 1.0, The Compliance Consortium, 2005. http://gilbane.com/publications /GRC_Operational_Approach_PD1_0_050512.pdf

[46] Also appears in "Enterprise Resilience: Risk and Security in the Networked World: A strategy+business Reader." Randall Rothenberg, ed.

[47] This site requires registration for a free membership.

[48] A description of The Balanced Scorecard and IT Governance is available at http://www.itgi.org/template_ITGI.cfm?template=/ContentManagement/ContentDisplay.cfm&ContentID=5550.

References

URLs are valid as of the publication date of this document.

[Alberts 02] Albert, Christopher & Dorofee, Audrey. *Managing Information Security Risks: The OCTAVE Approach*. Addison Wesley, July 2002.[49]

[Allen 02] Allen, Julia & Sledge, Carol. "Information Survivability: Required Shifts in Perspective." *CrossTalk*, July 2002. http://www.stsc.hill.af.mil/crosstalk/2002/07/allen.html.

[ACC 99] American Chemistry Council. Responsible Care® Guiding Principles, 1999. http://www.americanchemistry.com/.

[ACC 02] American Chemistry Council. *Implementation Guide for Responsible Care® Security Code of Management Practices: Site Security and Verification*, 2002. http://www.americanchemistry.com/.

[ACC 03] American Chemistry Council. *Responsible Care® Security Code of Management Practices*, 2003. http://www.americanchemistry.com/.

[Appel 04] Appel, Willie. "The ABC's of IT Governance: Practice 2273." Meta Group, October 2004. http://www.metagroup.com/us /displayArticle.do?oid=49863.

[Beauchamp 04] Beauchamp, Bob. "Mapping Out the Road to Compliance: It All Starts with Alignment." *Enterprise Leadership 2,* 3. BMC Software, 2004.

[Braithwaite 02] Braithwaite, Timothy. *Securing E-Business Systems: A Guide for Managers and Executives*. John Wiley & Sons, Inc., 2002.

[Braun 04] Braun, Robert & Stahl, Stan. "An Emerging Information Security Minimum Standard of Due Care." Citadel Information Group, Inc., 2004. http://www.citadel-information.com/min-std-due-care.pdf.

[49] Supporting publications can be found at http://www.cert.org/octave/pubs.html.

[BRT 04] Business Roundtable. "Securing Cyberspace: Business Roundtable's Framework for the Future." May 2004. http://www.businessroundtable.org/newsroom/Document.aspx?qs=55E6BF807822B0F12D0469167F75A70478252.

[BRT 05] Business Roundtable. "Committed to Protecting America: CEO Guide to Security Challenges." February 2005 (released May 2005). http://www.businessroundtable.org/publications/index.aspx.

[BSA 03] Business Software Alliance. "Information Security Governance: Toward a Framework for Action." October 2003. http://www.bsa.org/resources/loader.cfm?url=/commonspot/security/getfile.cfm&pageid=5841&hitboxdone=yes.

[Caralli 04a] Caralli, Richard. *The Critical Success Factor Method: Establishing a Foundation for Enterprise Security Management* (CMU/SEI-2004-TR-010). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2004. http://www.sei.cmu.edu/publications/documents/04.reports/04tr010.html.

[Caralli 04b] Caralli, Richard & Wilson, William. "The Challenges of Security Management." Carnegie Mellon University, Software Engineering Institute, July 2004. http://www.cert.org/archive/pdf/ESMchallenges.pdf.

[Caralli 04c] Caralli, Richard. *Managing for Enterprise Security* (CMU/SEI-2004-TN-046). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, December 2004. http://www.sei.cmu.edu/publications/documents/04.reports/04tn046.html.

[Caralli 05] Caralli, Richard & Parente, Amanda. "Enterprise Security Management: Refocusing Security's Role." news@sei, 2005, Number 1, Software Engineering Institute, Carnegie Mellon University, January 2005. http://www.sei.cmu.edu/news-at-sei/features/2005/1/feature-2-2005-1.htm.

[Carey 05] Carey, Mark. "Enterprise Risk Management: How To Jumpstart Your Implementation Efforts." International Risk Management Institute, 2005. http://www.irmi.com/Expert/Articles/2005/Carey02.aspx.

[Charette 05] Charette, Robert. Review comments, June 2005.

[CGTF 04] Corporate Governance Task Force. "Information Security Governance: A Call to Action." National Cyber Security Partnership, April 2004. http://www.cyberpartnership.org.

[CIMA 04] The Chartered Institute of Management Accountants. "Enterprise Governance – A CIMA Discussion Paper." 2004.[50]

[CISWG 04a] Corporate Information Security Working Group. Adam H. Putnam, Chairman; Subcommittee on Technology, Information Policy, Intergovernmental Relations & the Census Government Reform Committee, U.S. House of Representatives. "Report of the Best Practices Subgroup." March 3, 2004. http://reform.house.gov/TIPRC/News/DocumentSingle.aspx?DocumentID=3030.

[CISWG 04b] Corporate Information Security Working Group. Adam H. Putnam, Chairman; Subcommittee on Technology, Information Policy, Intergovernmental Relations & the Census Government Reform Committee, U.S. House of Representatives. "Report of the Best Practices and Metrics Teams." November 17, 2004; updated January 10, 2005. http://www.educause.edu/LibraryDetailPage/666&ID=CSD3661.

[CMMI 03] Capability Maturity Model® Integration. Carnegie Mellon University, Software Engineering Institute. http://www.sei.cmu.edu/cmmi/cmmi.html.[51]

[COSO 04] The Committee of Sponsoring Organizations of the Treadway Commission. "Enterprise Risk Management—Integrated Framework." September 2004.[52]

[CRS 04c] Moteff, John & Parfomak, Paul. "Critical Infrastructure and Key Assets: Definition and Identification." Order Code RL32631. Congressional Research Service, Library of Congress, October 1, 2004. http://www.fas.org/sgp/crs/RL32631.pdf.

[CRS 05] Fischer, Eric. "Creating a National Framework for Cybersecurity: An Analysis of Issues and Options." Order Code RL32777. Congressional Research Service, Library of Congress, February 22, 2005. http://www.thecre.com/pdf/secure/20050404_cyber.pdf.

[50] See also [IFAC 04]. http://www.cimaglobal.com/cps/rde/xbcr/SID-0AAAC544-D8A52CDB/live/enterprise_governance_DiscussionPaper_2004.pdf.

[51] Also Chrissis, Mary Beth, et al. *CMMI®: Guidelines for Process Integration and Product Improvement*. Addison Wesley, 2003.

[52] The executive summary and ordering information is available at http://www.coso.org.

[Dallas 04] Dallas, Susan & Bell, Michael. "The Need for IT Governance: Now More Than Ever (AV-21-4823)." Gartner, 20 January 2004.

[Drucker 04] Drucker, Peter. *The Daily Drucker: 365 Days of Insight and Motivation for Getting the Right Things Done.* HarperBusiness, 2004.

[FFIEC 02] Federal Financial Institutions Examination Council. *IT Examination Handbook: Information Security.* December 2002. http://www.ffiec.gov/ffiecinfobase/html_pages/it_01.html.

[FFIEC 04] Federal Financial Institutions Examination Council. *IT Examination Handbook: Management.* June 2004. http://www.ffiec.gov/ffiecinfobase/html_pages/it_01.html.

[Gartner 04] Hallawell, Arabella. "Gartner Global Security and Privacy Best Practices." Gartner Analyst Reports, March 16, 2004. Available at http://www.csoonline.com/analyst/report2332.html

[Geer 04a] Geer, Daniel E. "Why Information Security Matters." *Cutter Consortium Business-IT Strategies,* 7, 3. 2004.

[Geer 04b] Geer, Daniel E. "Security of Information When Economics Matters." Verdasys, May 2004. http://www.verdasys.com/pdfs/EconMatters.pdf.

[Gerdes 05] Gerdes, Michael. Review comments, June 2005.

[IIA 01] The Institute of Internal Auditors et al. "Information Security Governance: What Directors Need to Know." IIA, 2001. http://www.theiia.org/iia/index.cfm?doc_id=3061.

[IIA 05b] The Institute of Internal Auditors. "Global Technology Audit Guides: Change and Patch Management Controls: Critical for Organizational Success; Pre-release Draft." IIA, March 2005. http://www.theiia.org/index.cfm?doc_id=4706.

[IFAC 04] Professional Accountants in Business Committee; CIMA. "Enterprise Governance: Getting the Balance Right." International Federation of Accountants, February, 2004.[53] http://www.ifac.org/Store /Details.tmpl?SID=10770463423295840.

[53] See also [CIMA 04] and http://www.cimaglobal.com/cps/rde/xbcr /SID-0AAAC564-F335F3A9/live/enterprise_governance.pdf.

[ISO 00a] International Standards Organisation. ISO 9000:2000 *Quality Management Systems – Fundamentals and Vocabulary; Second Edition* 2000-12-15. ISO 9000:2000(E), 2000. [54]

[ISO 00b] International Standards Organization. ISO/IEC 17799 *Information Technology Code of Practices for Information Security Management, First edition*. ISO/IEC 17799:2000(E). December 2000.

[ISSA 04] Information Systems Security Association. "Generally Accepted Information Security Principles v3.0." http://www.issa.org/gaisp/gaisp.html (2005).

[ITGI 01] Information Technology Governance Institute.[55] "Information Security Governance: Guidance for Boards of Directors and Executive Management." Information Systems Audit and Control Foundation, 2001.

[ITGI 03] Information Technology Governance Institute. "Board Briefing on IT Governance, 2nd Edition." ITGI, 2003.

[ITGI 04] Information Technology Governance Institute. "COBIT Security Baseline: An Information Security Survival Kit." ITGI, 2004.[56]

[KPMG] KPMG. "Creating Stakeholder Value in the Information Age: The Case for Information Systems Governance." KPMG, 2004. http://www.kpmg.co.uk/services/ras/irm/isg.cfm.

[Lajoux 05] Lajoux, Alexandra. Review comments, May 2005.

[Matsuura 03] Matsuura, Jeffrey. "The Impact of National Infrastructure and Cyberspace Strategies on Legal Rights and Liabilities." University of Dayton School of Law, 2003. http://tprc.org/papers/2003/179/TPRC03matsuura.htm.

[McCollum 04] McCollum, Tim. "MacLean: Auditors Play Key Role Against IT Threats." *IT Audit 7*. Institute of Internal Auditors, May 2004. http://www.theiia.org/itaudit/index.cfm?fuseaction=forum&fid=5514.

[McMillan 05] McMillan, Robert. Review comments, May 2005.

---

[54] See also http://www.iso.org/iso/en/iso9000-14000/iso9000/qmp.html for a description of ISO 9000 quality management principles.

[55] http://www.itgi.org/

[56] Individual checklists are available at http://www.itgi.org.

[Moulton 03] Moulton, Rolf & Coles, Robert. "Applying information security governance." *Computers & Security 22* 7, Elsevier Ltd., 2003.

[NACD 01] National Association of Corporate Directors. "Information Security Oversight: Essential Board Practices." NACD, December 2001.[57]

[NACD 03] National Association of Corporate Directors. "Risk Oversight: Board Lessons from Turbulent Times." *Director's Monthly Newsletter, 27,* 1. NACD, January 2003.[58]

[NIST 96] Swanson, Marianne & Guttman, Barbara. "Generally Accepted Principles and Practices for Securing Information Technology Systems" (NIST Special Publication 800-14). National Institute of Standards and Technology, September 1996. http://csrc.nist.gov/publications/nistpubs/.

[NIST 04] Stoneburner, Gary, et al. "Engineering Principles for Information Technology Security (A Baseline for Achieving Security), Revision A" (NIST Special Publication 800-27 Rev A). National Institute of Standards and Technology. http://csrc.nist.gov/publications/nistpubs /800-27A/SP800-27-RevA.pdf (June 2004).

[OECD 02] Organisation for Economic Co-Operation and Development. "OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security." OECD, 2002. http://www.oecd.org /document/42/0,2340,en_2649_34255_15582250_1_1_1_1,00.html.

[OECD 04] Organisation for Economic Co-Operation and Development. "OECD Principles of Corporate Governance: 2004." OECD, 2004. http://www.oecd.org/document/49/0,2340,en_2649_34813_31530865 _1_1_1_1,00.html.

[Ponemon 04] Ponemon, Larry. "What Your CEO Thinks about Security (and How To Change IT)." *ComputerWorld*, 2004. http://www.computerworld.com /securitytopics/security/story/0,10801,96803,00.html.

[Posthumus 04] Posthumus, Shawn & von Solms, Rossouw. "A framework for the governance of information security." *Computers & Security 23*, 638-646, Elsevier, 2004.

[57] Ordering information is online at http://www.nacdonline.org/publications.

[58] Ordering information http://www.nacdonline.org/publications/.

[Scalet 05] Scalet, Sarah. "The Five Most Chocking Things About the ChoicePoint Debacle." *CSO Magazine*, May 2005. http://www.csoonline.com/read/050105/choicepoint.html.

[Slater 05] Slater, Derek. "Taking Leadership to a New Level." *CSO Magazine*, April 2005.[59] http://www.csoonline.com/read/041505/intro.html.

[Spafford 05] Spafford, George. Review comments, May 2005.

[Tarantino 04] Tarantino, Anthony. "The Impact of SOX and Corporate Governance on IT." *Executive Update 7* 18, Cutter Consortium, September 2004.

[Taylor 04a] Taylor, Patrick. "A Wake Up Call to All Information Security and Audit Executives: Become Business-Relevant." *Information Systems Control Journal 6.* (2004).

[Taylor 04b] Taylor, Jay. Review comments, December 2004.

[TechNet 03] TechNet. "Corporate Information Security Evaluation for CEOs – Preview Draft." December, 2003.[60]

[Tribbensee 03] Tribbensee, Nancy E. Ch. 4, "Liability for Negligent Security: Implications for Policy and Practice." 45-57. *Computer and Network Security in Higher Education* (Luker, Mark & Petersen, Rodney, Editors), EDUCAUSE Leadership Strategies, Jossey-Bass, Inc., 2003.

[Weill 04] Weill, Peter & Ross, Jeanne. *IT Governance: How Top Performers Manage IT Decision Rights for Superior Results*. Harvard Business School Press, 2004.

[Westby 04] Westby, Jody. "Information Security: Responsibilities of Boards of Directors and Senior Management." Testimony before the House Committee on Government Reform: Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, September 22, 2004. http://www.reform.house.gov/UploadedFiles/Westby1.pdf.

[Wheatley 04] Wheatley, Malcolm. "Security Sells." *CSO Magazine*, December 2004. http://www.csoonline.com/read/120104/sells.html.

[Zeichner 03] Zeichner, Lee. *Cyber Security & Corporate Liability*, Lexis-Nexis Publishing, 2003.

[59] Series of articles on security convergence, integrated security management, holistic security.

[60] The full TechNet evaluation is available at http://www.technet.org/cybersecurity/.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
(Leave Blank)	July 2005	Final

4. TITLE AND SUBTITLE	5. FUNDING NUMBERS
Governing for Enterprise Security	F19628-00-C-0003

6. AUTHOR(S)

Julia Allen

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213	CMU/SEI-2005-TN-023

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSORING/MONITORING AGENCY REPORT NUMBER
HQ ESC/XPK 5 Eglin Street Hanscom AFB, MA 01731-2116	

11. SUPPLEMENTARY NOTES

12A DISTRIBUTION/AVAILABILITY STATEMENT	12B DISTRIBUTION CODE
Unclassified/Unlimited, DTIC, NTIS	

13. ABSTRACT (MAXIMUM 200 WORDS)

Governing for enterprise security means viewing adequate security as a non-negotiable requirement of being in business. If an organization's management—including boards of directors, senior executives, and all managers—does not establish and reinforce the business need for effective enterprise security, the organization's desired state of security will not be articulated, achieved, or sustained. To achieve a sustainable capability, organizations must make enterprise security the responsibility of leaders at a governance level, not of other organizational roles that lack the authority, accountability, and resources to act and enforce compliance.

This technical report examines governance thinking, principles, and approaches and applies them to the subject of enterprise security. Its primary intent is to increase awareness and understanding of the issues, opportunities, and possible approaches related to treating security as a governance concern. In addition, this report identifies resources for enterprise security that leaders can use both within their organizations and with their networked partners, suppliers, and customers.

14. SUBJECT TERMS	15. NUMBER OF PAGES
computer security, corporate security, corporate computer security, management, enterprise management, security, security practice	81

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL