Governing for Enterprise Security (GES)

Implementation Guide

Article 1: Characteristics of Effective Security Governance[1]

Julia H. Allen, Carnegie Mellon University, Software Engineering Institute, CERT®

Jody R. Westby, CEO, Global Cyber Risk LLC
Adjunct Distinguished Fellow, Carnegie Mellon CyLab

February 2007

[1] Much of the content in this article is excerpted and updated from previously published work [Allen 05, Allen 06a, Allen 06b, Allen 06c].

Abstract: This article sets the stage for the Governing for Security Implementation Guide series. It first presents several key definitions for enterprise governance, IT governance, and security governance. It describes eleven characteristics intended to answer the question "How would I know effective security governance if I saw it?" The article goes on to compare and contrast both effective and ineffective security governance actions and then describes ten key challenges that leaders need to anticipate and address.

Introduction

This article (and subsequent articles in this series) builds upon established definitions of enterprise governance and IT governance. It then extends and interprets these to explain governance of enterprise security programs (ESP) that protect digital[2] assets and business operations.

A well-accepted definition of *enterprise governance* as set forth by the International Federation of Accountants (IFAC) and the Information Systems Audit and Control Association (ISACA) is as follows:

> Enterprise governance is 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 organization's resources are used responsibly [IFAC 04].

The Business Roundtable has determined that effective enterprise governance includes [BRT 05]:

- setting the culture and managerial tone for the conduct of the entity being governed
- specifying a framework for decision making, accountability, and integrity, including assigned roles and responsibilities and codes of conduct
- determining a clear, strategic direction for the organization with defined goals
- directing, controlling, and strongly influencing the entity to achieve stated expectations
- producing financial statements that accurately present the conditions and results of operations and making timely disclosures
- aligning risk management with strategy and ensuring compliance

[2] This guide does not specifically address the security or protection of physical assets such as facilities, equipment, and information in physical form, although many of the guidelines are applicable for these types of assets.

- conducting effective due diligence and audits of operations and managerial practices
- assuring that decisions are implemented as intended through effective controls, metrics, and enforcement policies
- making governance systemic throughout the organization

Governance extends to the management of an organization’s use of IT. The IT Governance Institute declares that [ITGI 03]:

> *IT governance* is the responsibility of the board of directors and executive management. It is an integral part of enterprise governance and consists of the leadership and organizational structures and processes that ensure that the organization’s IT sustains and extends the organization’s strategies and objectives.

Enterprise governance and IT governance increasingly encompass the security of IT systems and information. Members of the American Society for Industrial Security (ASIS), the Information Systems Security Association (ISSA), and ISACA (with Booz Allen Hamilton) examined the convergence of security risks and the business operations. In their report, *Convergence of Enterprise Security Organizations,* they adopt the ASIS description of this convergence [AESRM 05]:

> [T]he identification of security risks and interdependencies between business functions and processes within the enterprise and the development of managed business process solutions to address those risks and interdependencies.

Governing for enterprise security is defined as [Allen 05]:

- directing and controlling an organization to establish and sustain a culture of security in the organization’s conduct (beliefs, behaviors, capabilities, and actions)
- treating adequate security as a non-negotiable requirement of being in business

In its publication, *Information Security Handbook: A Guide for Managers* [Bowen 06], the U.S. National Institute of Standards and Technology (NIST) expands this definition for *information security governance* as follows:

> . . . the process of establishing and maintaining a framework and supporting management structure and processes to provide assurance that information security strategies
>
> - are aligned with and support business objectives
> - are consistent with applicable laws and regulations through adherence to policies and internal controls
> - provide assignment of responsibility
>
> all in an effort to manage risk.

Governance and management of security are most effective when they are systemic — woven into the very culture and fabric of organizational behaviors and actions. In this regard, culture is defined as the predominant, shared attitudes, values, goals, behaviors, and practices that characterize the functioning of a group or organization. Culture thereby creates and sustains connections among policies, processes, people, and performance. Effective security should be thought of as an attribute or characteristic of an organization. It becomes evident when everyone proactively carries out their roles and responsibilities, creating a culture of security that displaces ignorance and apathy.

To this end, security must come off the technical sidelines as activities and responsibilities solely relegated to software development and IT departments. Today, boards of directors, senior executives, and managers all must work to establish and reinforce a relentless, ongoing drive toward effective enterprise security. If the responsibility for enterprise security is assigned to roles that lack the authority, accountability, and resources to implement and enforce it – and which do not have organizational connection points horizontally and vertically throughout the organization – the desired level of security will not be articulated, achieved, or sustained.

Contrary to popular belief that security is a technical issue, even the best efforts to buy software-based security solutions and build security into developed software and operational systems encounter "considerable resistance because the problem is mostly organizational and cultural, not technical" [Steven 06]. Effective security in today's interconnected environment requires integrating legal, managerial, operational, and technical considerations.

This shift in perspective elevates security from a standalone, technical concern to an enterprise issue. Because security is now a business problem[3], the organization must activate, coordinate, deploy, and direct many of its core resources and competencies so security risks are managed and aligned with the entity's strategic goals, operational criteria, compliance requirements, and technical system architecture. To *sustain* enterprise security, the organization must move toward a security management process that is strategic, systematic, and repeatable, with efficient use of resources and effective, consistent achievement of goals [Caralli 04]. Such a process needs to account for the fact that policies, procedures, and technologies are dynamic.

This article describes ways to determine if security is being effectively addressed as a governance concern. It compares and contrasts effective with ineffective practices, and it describes some of the challenges that need to be met to ensure a successful security program.

[3] See also "Governing for Enterprise Security" [Allen 05] and "Security Is Not Just a Technical Issue. [Allen 06b]"

Eleven Characteristics of Effective Security Governance

One of the best measures that an organization is addressing security as both a governance and management concern is that leaders regularly promulgate a set of beliefs, behaviors, capabilities, and actions that are consistent with security best practices and standards. These measures aid in building a security-conscious culture. They can be expressed as statements about the organization's current behavior and condition as follows:

An Enterprise-wide Issue

Security is managed as an enterprise issue, horizontally, vertically, and cross-functionally throughout the organization. The scope of an Enterprise Security Program (ESP) as described here includes people, products, plants, processes, policies, procedures, systems, technologies, networks, and information (P6STNI) [Westby 05].

Leaders are Accountable

Executive leaders understand their accountability and responsibility with respect to security for the organization, for their stakeholders, for the communities they serve (including the internet community), and for the protection of critical national infrastructures as well as economic and national security interests.

Senior leaders visibly engage in the management and oversight of the enterprise security program and support this work with adequate financial resources, effective management, risk-based policies, and annual reviews and audits. Business executives accept responsibility and ownership for the security risks associated with their digital assets (systems, networks, applications, information).

Viewed as a Business Requirement

Security is viewed as a business requirement that directly aligns with strategic goals, enterprise objectives, risk management plans, compliance requirements, and top-level policies. Managers across the enterprise understand how security serves as a business enabler. “Implementation of an effective security program is ultimately a matter of enlightened organizational self-interest” [BSA 03].

Security is considered as a cost of doing business and an investment rather than an expense or a discretionary budget-line item. Security policy is set at the top of the organization and business units and staff are not allowed to decide unilaterally how much security they want. This said, appropriate policy exception processes allow the business to continue, while ensuring that leaders have adequate oversight. Adequate and sustained funding and allocation of adequate security resources are a given.

Risk-based

Determining how much security is enough is based upon the risk exposure an organization is willing to tolerate, including compliance and liability risks, operational disruptions, reputational harm, and financial loss. Exposure to reasonably foreseeable internal and external risks is examined and tolerance levels are reset if necessary, as part of the normal process of reviewing organizational performance and risks.

Roles, Responsibilities, and Segregation of Duties Defined

Qualified personnel are assigned to leadership positions – Chief Information Officer (CIO), Chief Information Security Officer (CISO) and/or Chief Security Officer (CSO),[4] Chief Risk Officer (CRO), and Chief Privacy Officer (CPO). Security roles and responsibilities for business leaders are denoted by separate lines of reporting and a clear delineation of responsibilities that take into account segregation of duties, accountability, and risk management.

Addressed and Enforced in Policy

Security requirements are implemented through well-articulated policies and procedures which are supported by people, procedural, and technical solutions including controls, training, monitoring, and enforcement. Rewards, recognition, and consequences with respect to security policy compliance are consistently applied and reinforced.

Adequate Resources Committed

Key personnel, including IT and security staff, have adequate resources, authority, and time to build and maintain core competencies in enterprise security. This includes the use of security experts, the deployment of technologies, and ongoing education regarding threats, vulnerabilities, and risks to business continuity.

Staff Aware and Trained

All personnel who have access to digital assets understand their daily responsibilities to protect and preserve the organization’s security posture. Awareness, motivation, and compliance are the accepted, expected cultural norm. Security awareness and targeted training are conducted routinely and consistently, and security responsibilities are reflected in job descriptions.

A Development Life Cycle Requirement

Security requirements are addressed throughout all system/software development life cycle phases including acquisition, initiation, requirements engineering, system architecture and design, development, testing, operations, maintenance, and retirement.

[4] Some organizations have both a CSO and CISO, with a separation of duties between facilities and personnel security, and information/IT security. As organizations realize, however, that the security of their physical facilities, processes, and personnel is impacted by IT systems and devices, and vice versa, they are integrating the CISO and CSO responsibilities into either a consolidated CSO position or into the Chief Risk Officer (CRO) role [ITCI 06]. This guide uses the term CSO, but this role is intended to encompass the CISO and could be replaced by the CRO. Alternatively, if an organization has both a CSO and CRO, they both participate in the development and sustainment of the ESP, with the CSO taking the lead in implementing the security requirements of the risk management plan, with oversight by the CRO.

Planned, Managed, Measurable, and Measured

Security is considered an integral part of normal strategic, capital, and operational planning cycles. Security has achievable, measurable objectives that are integrated into strategic and operational plans, and implemented with effective controls and metrics. Reviews and audits of plans identify security weaknesses and deficiencies, requirements for the continuity of operations, and measure progress against plans of action and milestones (POAMs).

Senior leaders measure this work against defined performance parameters. Managers view security as one of their responsibilities and understand that their team’s performance with respect to security is measured as part of their overall performance.

Security is actively considered as part of any new project initiation, acquisition, or relationship, and as part of ongoing project management.

Reviewed and Audited

The board risk and audit committees conduct regular reviews and audits of the ESP. They ensure that all components of the program are maintained and that the ESP continues to sustain the desired state of security for the organization.

Effective versus Ineffective Security Governance[5]

Comparing and contrasting a set of behaviors and actions is useful to further illustrate effective versus ineffective security governance. Sometimes the absence of a quality, value, or cultural norm is a more revealing indicator than its presence. Table 1 presents such a comparison from different perspectives within an enterprise.

Table 1: Effective versus Ineffective Security Governance

Effective	Ineffective or Absent
Board members understand that information security is critical to the organization and demand to be updated quarterly on security performance and breaches. The board establishes a board risk committee (BRC) that understands security's role in achieving compliance with applicable laws and regulations, and in mitigating organization risk. The BRC conducts regular reviews of the ESP. The board's audit committee (BAC) ensures that annual internal and external audits of the security program are conducted and reported.	Board members do not understand that information security is in their realm of responsibility, and focus solely on corporate governance and profits. Security is addressed adhoc, if at all. Reviews are conducted following a major incident, if at all. The BAC defers to internal and external auditors on the need for reviews. There is no audit plan to guide this selection.
The BRC and executive management team set an acceptable risk level. This is based on comprehensive and periodic risk assessments that take into account reasonably foreseeable internal and external security risks and magnitude of harm. The resulting risk management plan is aligned with the entity's strategic goals, forming the basis for the company's security policies and program.	The CISO locates boilerplate security policies, inserts the organization's name, and has the CEO sign them. If a documented security plan exists, it does not map to the organization's risk management or strategic plan, and does not capture security requirements for systems and other digital assets.
A cross-organizational security team	CEO, CFO, general counsel, HR, procurement

[5] This builds upon and modifies a similar presentation found in an article by Harris [Harris 06].

Effective	Ineffective or Absent
comprised of senior management, general counsel, CFO, CIO, CSO and/or CRO, CPO, HR, internal communication/public relations, and procurement personnel meet regularly to discuss the effectiveness of the security program, new issues, and to coordinate the resolution of problems.	personnel, and business unit managers view information security as the responsibility of the CIO, CISO, and IT department and do not get involved. The CSO handles physical and personnel security and rarely interacts with the CISO. The general counsel rarely communicates particular compliance requirements or contractual security provisions to managers and technical staff, or communicates on an ad-hoc basis.
The CSO/CRO reports to the COO or CEO of the organization with a clear delineation of responsibilities and rights separate from the CIO. Operational policies and procedures enforce segregation of duties (SOD) and provide checks and balances and audit trails against abuses.	The CISO reports to the CIO. The CISO is responsible for all activities associated with system and information ownership. The CRO does not interact with the CISO or consider security to be a key risk for the organization. (See also footnote 3.)
Risks (including security) inherent at critical steps and decision points throughout business processes are documented and regularly reviewed. Executive management holds business leaders responsible for carrying out risk management activities (including security) for their specific business units. Business leaders accept the risks for their systems and authorize or deny their operation.	All security activity takes place within the security department, thus security works within a silo and is not integrated throughout the organization. Business leaders are not aware of the risks associated with their systems or take no responsibility for their security.
Critical systems and digital assets are documented and have designated owners and defined security requirements.	Systems and digital assets are not documented and not analyzed for potential security risks that can affect operations, productivity, and profitability. System and asset ownership are not clearly established.

Effective	Ineffective or Absent
There are documented policies and procedures for change management at both the operational and technical levels, with appropriate segregation of duties. There is zero tolerance[6] for unauthorized changes with identified consequences if these are intentional.	The change management process is absent or ineffective. It is not documented or controlled. The CIO (instead of the CISO) ensures that all necessary changes are made to security controls. In effect, SOD is absent.
Employees are held accountable for complying with security policies and procedures. This includes reporting any malicious security breaches, intentional compromises, or suspected internal violations of policies and procedures.	Policies and procedures are developed but no enforcement or accountability practices are envisioned or deployed. Monitoring of employees and checks on controls are not routinely performed.
The ESP implements sound, proven security practices and standards necessary to support business operations.	No or minimal security standards and sound practices are implemented. Using these is not viewed as a business imperative.
Security products, tools, managed services, and consultants are purchased and deployed in a consistent and informed manner, using an established, documented process. They are periodically reviewed to ensure they continue to meet security requirements and are cost effective.	Security products, tools, managed services, and consultants are purchased and deployed without any real research or performance metrics to be able to determine their ROI or effectiveness. The organization has a false sense of security because it is using products, tools, managed services, and consultants.
The organization reviews its enterprise security program, security processes, and security's role in business processes. The goal of the ESP is continuous improvement.	The organization does not have an enterprise security program and does not analyze its security processes for improvement. The organization addresses security in an ad-hoc fashion, responding to the latest threat or attack, often repeating the same mistakes.

[6] Zero tolerance means that systems are regularly monitored for unauthorized changes. If discovered, such changes are immediately investigated or backed out of operational configurations and a post mortem review is performed to ensure this does not recur. Refer to "Prioritizing IT Controls for Effective, Measurable Security. [Kim 06]"

Effective	Ineffective or Absent
Independent audits are conducted by the BAC. Independent reviews are conducted by the BRC. Results are discussed with leaders and the Board. Corrective actions are taken in a timely manner, and reviewed.	Audits and reviews are conducted after major security incidents, if at all.

Ten Challenges to Implementing an Enterprise Security Program

Launching an enterprise security program and taking the governance actions necessary to sustain it requires tenacity and perseverance. Organizations may expect to encounter significant challenges along the way. Due to the enterprise nature of these programs, these challenges may occur at all levels of the organization and throughout all phases of the ESP. Understanding them and anticipating how to respond greatly facilitates the process as well as the effectiveness of the ESP.

The good news is that challenges, once mastered, can become opportunities. Leaders who effectively address these challenges can create business opportunities by capitalizing on successful solutions and creating a trusted environment for customers, business partners, and employees.

Challenges to consider often include

- understanding the implications of ubiquitous access and distributed information
- appreciating the enterprise-wide nature of the security problem
- overcoming the lack of a game plan
- establishing the proper organizational structure and segregation of duties
- understanding complex global legal compliance requirements and liability risks
- assessing security risks and the magnitude of harm to the organization
- determining and justifying appropriate levels of resources and investment
- dealing with the intangible nature of security
- reconciling inconsistent deployment of security best practices and standards
- overcoming difficulties in creating and sustaining a security-aware culture

Ubiquitous Access, Distributed Information

Many boards and executives do not understand the globally connected nature of the internet and how this facilitates access to information distributed throughout an organization and its partner and customer base. Risks and opportunities increasingly derive from who you are connected to (your systems and networks) and who is connected to you.

Robert Metcalfe, the “father of the ethernet,” has postulated that the value of the network increases at a square of the number of nodes on the net. It is likely that risk increases at an even higher exponent in the world we have today with the internet, where one may essentially reach all. Borders, assuming they exist at all, have been greatly extended whether intended or not.

Today’s marketplace is driven by consumers who have ready and direct access to whomever they wish to transact business with around the world, and who have the option to change their choices with great ease for any reason. Sometimes the needs and requirements of the customer base are different from – or possibly even at odds with – the identified or stated needs and requirements of the business. This creates conflicts and security risks that are important to understand and mitigate.

For example, the need to protect access to sensitive information using strong and multiple layers of authentication and access controls is a business requirement. The need to provide easy and fast access to such information to transact business may be a customer, partner, or supplier requirement. The tension between business and customer requirements is often reconciled under the presumption that both sides have gone through the process of identifying sensitive information and categorizing it according to a classification scheme to reach an accommodation in terms of levels of protection. Unfortunately, this is often not the case.

Enterprise-wide Nature of Security

Security must support and protect business processes. Understanding the full breadth and reach of security requires education. Those responsible for security often find that it can be difficult to persuade senior leaders of the need to implement enterprise security in a systemic way. For most organizations and people, security, like insurance, can be an abstract concept, concerned with hypothetical events that may never occur.

Security responsibilities are distributed throughout an organization, requiring cross-organizational interaction, cooperation, and execution. It cannot be contained or delegated to a specific function or department within an organization or treated as solely a technical problem. Without a clear understanding of enterprise security, the people and processes that play an essential role may be easily missed. Many functions and departments within the organization need to interact to create and sustain an effective security solution that includes strategic, legal, technological, organizational, economic, and social considerations. [Westby 05]

At the technical level, this includes making sure security is adequately addressed through the entire system development lifecycle, including phases involving requirements, design, and development or acquisition of software-based systems, rather than waiting until the system is deployed. [Bowen 06]

Lack of a Game Plan

Leaders often do not know where or how to start. They lack a framework for action – how to set priorities, assign tasks, get started, and monitor implementation.
There are now internationally-accepted approaches to enterprise security that can help organizations determine what should be done and who should do it. There is guidance, such as that offered within this series of articles, that can help boards and executives better understand how to approach enterprise security. Without such an approach, leaders are unclear regarding how to assign responsibilities, allocate security funding, determine return on investment, and measure performance [BSA 03, Westby 04b].

Organizational Structure and Segregation of Duties

Leaders have often allocated security responsibilities in an ad hoc manner, with many erroneously placing it within the realm of the chief information officer (CIO). If a chief information security officer (CISO) is appointed, often that role reports to the CIO, violating segregation of duties (SOD) principles. The CIO and CISO often have conflicting demands with regard to IT functionality and costs, and they may not be in a position to leverage the resources and authority necessary to address security issues across multiple business lines or divisions. Because little attention is usually given to this issue at the CEO or board level, information security efforts are frequently undercut by the wrong organizational structure [BSA 03, CGTF 04].

Given the close alignment of operational IT and operational security concerns, some organizations may initially have the CISO reporting to the CIO. In this case, however, segregation of duties needs to be explicitly addressed to avoid conflicts of interest. This includes the possible allocation of resources to IT operational activities at the expense of security needs, and sending a message that security is not a high priority resulting in a weakened culture of security.

Complex Global Legal Framework

Enterprise security requirements can flow from a wide range of international, national, state, and local laws and regulations, as well as international standards, policies, and legal contracts. Increasingly, privacy and security requirements around the globe are conflicting or, at best, create multiple layers of differing requirements [Smedinghoff 06, Westby 04a]. “Organizations may be faced with the challenge of implementing different compliance measures” and having to monitor these measures to meet a range of reporting requirements [Bowen 06]. In addition, this regulatory landscape is always changing so security programs need to be reviewed and adjusted on a regular basis to ensure they meet current compliance requirements and keep potential liabilities in check.

Understanding privacy and security requirements is further complicated by the difficulty in accommodating cross-border data flows and meeting compliance requirements of security breach notification and data retention laws. Additionally, vastly differing laws regarding cyber criminal activities create further complexities that must be woven into the ESP. [Westby 03]

Understanding Security Risks

Security activities are often under-funded in proportion to the risk and magnitude of the harm that incidents could produce because the security responsibilities are not properly aligned with business operations and risks. Determining the right level of security is a business decision based on the outcomes of an effective risk assessment. Such an assessment includes an analysis of the foreseeable internal and external risks and the magnitude of harm associated with them. It is important that boards and executives draw on established guidance in assessing risks and understand the harm that could flow to their organization from them [Bowen 06, BSA 03, Stoneburner 02]. When effectively overcome, security risks can also represent opportunities that may preserve and enhance business value and create marketplace advantage.

Cost/Benefit Not Easily Quantifiable

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

The benefits of security investments 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? This difficulty has dogged not only security but also efforts to improve software quality, conduct proper testing, keep documentation up to date, maintain current configuration and hardware/software inventory records, and the like [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.

That said, organizations such as the congressional research service have documented useful guidance and statistics on losses associated with security events [CRS 04]. They state:

> Investigations into the stock price impact of cyber-attacks show that identified target firms suffer losses of one to five percent in the days after an attack. For the average New York Stock Exchange corporation, price drops of these magnitudes translate into shareholder losses of between $50 million and $200 million.

The Effects of Security Are Often Intangible

While the tangible effects of a security incident can be measured (in terms of lost productivity and staff time to recover and restore systems), the intangible effects can be an order of magnitude larger. Intangible effects include the impact on an organization’s trust relationships, harm to its reputation, and loss of economic and societal confidence resulting from a publicly reported breach.

In terms of its inherent nature, security is sometimes described as an emergent property of networks and the organizations they support. Given security's many dimensions, the precise location where security is enacted cannot be readily identified. An organization's security condition is often determined in the interaction and intersection of people, processes, and technology. As the organization and the underlying network infrastructure change in response to the evolving risk environment, so will the state of an entity’s security.

Inconsistent Deployment of Best Practices and Measures

Many organizations do not approach security by deploying sound, commonly accepted practices; rather, they fix problems as they occur and try to keep up with the security risks that accompany change and growth. As a result, establishing an ESP can be an especially daunting task.

Fortunately, there are several widely accepted security best practices and standards. The International Organization for Standardization (ISO) leads the way with ISO 17799 [ISO 05a] and ISO 27001 [ISO 05b]. The National Institute of Standards & Technology has published a series of world-class standards and information security guidance that is applicable to both public and private sector entities.

Professional and technical associations have developed best practices that have been adopted globally by both industry and government. A good example is the Control Objectives for Information and related Technology (CobiT) framework, developed by the Information Systems and Audit Control Association [ITGI 05b]. A growing number of guidelines and checklists, such as those created by the Center for Internet Security, identify practices that are considered acceptable by most professionals. [Allen 06d].

Without question, the security situation organizations face today is, in part, due to the lack of attention given these practices and standards. This shortfall is evidenced by the number of vulnerabilities reported to CERT[7], many of which have known solutions that have not been implemented. Implementing sound practices and security standards can significantly advance an organization's state of security when properly deployed as part of an ESP. That said, not every practice and standard applies to every organization. Leaders need to ensure that practice selection and implementation directly support business objectives.

Difficulties in Creating and Sustaining a Culture of Security

Achieving a particular state of security is no guarantee that it can be sustained. Security is not a one-time project with a beginning and an end; it is an ongoing process. It requires continuous improvement, monitoring, measuring, and executing (i.e. "doing") [Allen 06e, ISO 05b]. Continuous improvement requires attention and investment, and security investments often come at the expense of other priorities in terms of accounting and economic opportunity.

Security is hard, often annoying, and something most people and organizations would rather not deal with. There are formidable disincentives to addressing security at more than just a tactical, technical level. As a networked community, there is no perfect solution to effective security, and measures and benchmarks can vary from industry to industry and company to company. This situation is difficult to improve without a significant increase in the reporting of incident cost/loss metrics to estimate probable losses that would have occurred had steps not been taken to reduce risk exposure. Such metrics are analogous to insurance actuarial data, which provides a statistical basis for estimates of loss [Gerdes 05].

Furthermore, security safeguards are 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 04]. The board and senior leadership should require formal audits and reviews of the security program, with a formal report card and timely closure of corrective actions.

Therefore, the board and senior management have a difficult task in setting the tone for security and creating a culture of security awareness with motivation to adhere to security requirements. Policies are not enough; they must be supported with actions from the top that relay the importance of security to corporate operations and competitiveness, and convey the impact that security breaches will have on corporate profits and reputation.

[7] CERT and CERT Coordination Center are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

This is most effectively done through the development and sustainment of an ESP with active and visible senior leadership involvement [Westby 04b].

Summary

Understanding – and overcoming – challenges facing organizations as they develop and sustain an ESP is part of the process on the path to effective security. Each challenge requires the attention of multiple players within an organization. Thus, challenges can be used as a unifying mechanism through the work of a cross-organizational security team and can help develop buy-in from operational personnel as they contribute to security solutions.

An effective approach to governing and managing enterprise security must confront these challenges head-on, offering counterpoints and benefits to anticipate and offset each challenge. Increasing awareness, knowledge, and understanding of security are necessary first steps toward changing common beliefs. This includes framing the security value proposition to include risk and opportunity.

Conclusion

In today's economic, political, technological, and social environment, addressing security is 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. Domestic and foreign laws and 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 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.

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.

References for this article are available at http://www.cert.org/governance/references.html.