This document is part of the US-CERT website archive. These documents are no longer updated and may contain outdated information. Links may also no longer function. Please contact info@us-cert.gov if you have any questions about the US-CERT website archive.

Security Is Not Just a Technical Issue

Published: November 30, 2009 | Last revised: May 13, 2013

Author(s): Julia H. Allen

Maturity Levels and Audience Indicators: L3 / E L M

SDLC Life Cycles: Management

Abstract

Updates to this material are, in part, either adapted or excerpted from *Software Security Engineering: A Guide for Project Managers* [Allen 2008].

This overview defines the scope of governance concern as it applies to security. It describes some of the top-level considerations and characteristics to use as indicators of a security conscious culture and whether an effective program is in place.

Security's days as just a technical issue are done. It is becoming a central concern for leaders at the highest level of many organizations and governments, transcending national borders. Customers are demanding it as worries about privacy, the protection of personally identifiable information, and identity theft grow. Business partners, suppliers, and vendors are requiring it from one another, particularly when providing mutual network and information access. Networked efforts to steal competitive intelligence and engage in extortion are becoming more prevalent. Security breaches and data disclosure increasingly arise from criminal behavior motivated by financial gain.

Current and former employees and contractors who have or had authorized access to their organization's system and networks are familiar with internal policies, procedures, and technology and can exploit that knowledge to facilitate attacks and even collude with external attackers. Malicious insider acts that need to be mitigated include sabotage, fraud, theft of confidential or proprietary information, and potential threats to our nation's critical infrastructure. Recent CERT research documents cases of successful insider incidents during the software development life cycle.[1]

According to the IT Governance Institute ". . . boards of directors will increasingly be expected to make information security an intrinsic part of governance, integrated with processes they already have in place to govern other critical organizational resources" [ITGI 2006]. Ultimately, directors and senior executives set the direction for how enterprise security (including software security) is perceived, prioritized, managed, and implemented. This is governance in action.[2]

The Business Roundtable (an association of chief executive officers of leading U.S. companies) asserts the following in its report Committed to Protecting America: CEO Guide to Security Challenges:

> 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 [BRT 2005].

As additional evidence of this growing trend, the Deloitte 2007 Global Security Survey of top global financial services institutions states the following:

> Information security is no longer a technology-focused problem. It has become the basis for business survival as much as any other issue. A key finding shows that 81% of respondents, many more than in studies of previous years, feel that the issue of security has risen to the level of the C-suite or board as an issue of critical concern.

> Information Security Governance is a framework predicated on principles and accountability requirements that encourage desirable behavior in the application and use of technology. Results from the present study indicate 81% of respondents have a defined information security governance structure (e.g., defined responsibilities, policies, and procedures) while 18% are in the process of establishing one [Deloitte 2007].

According to the Building Security In Maturity Model, “Executives and middle management, including line of business owners and product managers must understand how early investment in security design and security analysis affects the degree to which users will trust their products. Business requirements should explicitly address security needs. Any sizeable business today depends on software to work. Software security is a business necessity” [McGraw 2009].

While there is growing evidence that senior leaders are paying more attention to the risks and business implications associated with poor or inadequate security governance (refer to Maturity of Practice), a recent Carnegie Mellon University survey indicates that there is much work to be done:

> Survey results confirmed the belief among IT security professionals that boards and senior executives are not adequately involved in key areas related to the governance of enterprise security. Of the pool of respondents, only 36% of them indicated that their board had direct involvement with oversight of information security.
>
> The respondents indicated that the vast majority of boards that are reviewing privacy and security issues are not focusing on important activities that could help protect the organization from high risk areas, such as reputational or financial losses flowing from breaches of personally identifiable information [Westby 2008].

Governance and Security

Governance means setting clear expectations for business conduct and then following through to ensure the organization fulfills those expectations. Governance action flows from the top of the organization to all of its business units and projects. Done right, governance enables an organization's approach to nearly any business problem, including security. National and international regulations call for organizations—and their leaders—to demonstrate due care with respect to security. This is where governance can help.

Moreover, organizations are not the only entities that will benefit from strengthening enterprise security through clear, consistent governance. Ultimately, entire nations will benefit. "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 2004].

efinitions of Security Governance

The term *governance* applied to any subject can have a wide range of interpretations and definitions. For the purpose of this chapter, we define governing for enterprise security[3] as [Allen 2005]

> 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 2006], NIST (National Institute of Standards and Technology) defines information security governance in greater detail:

> . . . 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, and
  - provide assignment of responsibility

> all in an effort to manage risk.

In his article "Adopting an Enterprise Software Security Framework," John Steven states

> In the context of an Enterprise Software Security Framework, governance is competency in measuring software-induced risk and supporting an objective decision-making process for remediation and software release. This competency involves creating a seat at the project management table for software risk alongside budget and scheduling concerns [Steven 2006]. (See also the BSI Project Management content area.)

In the context of security, governance incorporates a strong focus on risk management. Governance is an expression of responsible risk management, and effective risk management requires efficient governance. One way governance manages risk is to specify a framework for decision making. It makes clear who is authorized to make decisions, what the decision making

rights are, and who is accountable for decisions. Consistency in decision making across an enterprise[4] , a business unit, or a project boosts confidence and reduces risk.

Duty of Care

In the absence of some type of meaningful governance structure and way of managing and measuring enterprise security, the following questions naturally arise. *Organization* can include an entire enterprise, a business or operating unit, or a project.

- 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 that require business-continuity, crisis-management, and disaster-recovery actions?
  - to protect stakeholder interests and meet stakeholder expectations?
  - to comply with regulatory and legal requirements?
  - to develop, acquire, deploy, operate, and use application software and software-intensive systems?
  - to ensure enterprise viability?

Art Coviello, co-chair of the Corporate Governance Task Force,[5] 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."[6]

As a result, director and officer oversight of corporate digital security (including software security) is embedded within the duty of care[7] owed to enterprise shareholders and stakeholders. Leaders who hold equivalent roles in government, non-profit, and educational institutions need to view their responsibilities similarly.

Leading by Example

Demonstrating duty of care with respect to security is a tall order, but leaders must be up to the challenge. 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 worth their own time and attention. In this way, a security-conscious culture can grow.

It seems clear that boards of directors, senior executives, business unit and operating unit, and project managers all must play a role in making and reinforcing the business case for effective enterprise security. Trust, reputation, brand, stakeholder value, customer retention, and increased operational costs are all at stake if security governance and management are performed poorly. Organizations will be much more competent in using security to mitigate risk if their leaders treat it as essential to the business and are aware and knowledgeable about security issues.

Characteristics of Effective Security Governance and Management

One of the best measures that an organization is addressing security as a governance and management concern is a consistent and reinforcing 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.[8] They can be expressed as statements about the organization's current behavior and condition.[9]

- Security is managed as an enterprise issue, horizontally, vertically, and cross-functionally throughout the organization. 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 and economic and national security interests.
- Security is treated as a business requirement. It is considered a cost of doing business and an investment rather than an expense or discretionary budget-line item. Security policy is set at the top of the organization with input from key stakeholders. Business units and staff are not allowed to decide unilaterally how much security they want. Adequate and sustained funding and allocation of adequate security resources are a given.
- Security is considered an integral part of normal strategic, capital, project, and operational planning cycles. Security has achievable, measurable objectives that are integrated into strategic and project plans and implemented with effective controls and metrics. Reviews and audits of plans identify security weaknesses and deficiencies as well as requirements for the continuity of operations. They measure progress against plans of action and milestones. Determining how much security is enough equates to how much risk exposure an organization can tolerate.
- Security is addressed as part of any new project initiation, acquisition, or relationship and as part of ongoing project management. 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.
- Managers across the organization understand how security serves as a business enabler (versus an inhibitor). They 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.
- All personnel who have access to digital assets and enterprise networks understand their individual responsibilities with respect to protecting and preserving the organization's security, including the systems and software that it uses and develops. Awareness, motivation, and compliance are the accepted, expected cultural norm. Rewards, recognition, and consequences with respect to security policy compliance are consistently applied and reinforced.

Leaders who are committed to dealing with security at a governance level can use this checklist to determine the extent to which a security-conscious culture is present (or needs to be present) in their organizations. The relative importance of each statement depends on the organization's culture and business context.

Two Examples of Security Governance

Payment Application Data Security Standard (PA-DSS)

The existence and enforcement of the Payment Card Industry (PCI) Data Security Standard (DSS) [PCI 2009a] represent a demonstrable act of governance by the payment card industry over its members and merchants. This standard presents a comprehensive set of twelve requirements for enhancing payment account data security. It "is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures."[10] This standard is summarized in Plan, Do, Check, Act.

An additional standard that is part of the PCI DSS standards suite is the Payment Application Data Security Standard (PA-DSS). PA-DSS specifically addresses software security. Its purpose is to assist software vendors of payment applications to develop and deploy products that are more secure, protect cardholder data, and are compliant with the broader PCI standard.

All fourteen PA-DSS practice descriptions include detailed subpractices and testing procedures for verifying that the practice is in place [PCI 2009b]. The PCI Standards Council maintains a list of validated payment applications that meet this standard. Payment card merchants can use it to select applications that better ensure the protection of cardholder data.

The American Chemistry Council

The American Chemistry Council's website describes the organization as follows:

> The American Chemistry Council represents the companies that make the products that make modern life possible, while working to protect the environment, public health, and the security of our nation. Founded in 1872, our support for research and initiatives that serve our communities and customers continues to this day. Our member companies have committed to implement a set of goals and guidelines that go above and beyond federal regulation on health, safety, security and the environment.

Security governance in action can be inspiring. The American Chemistry Council's Responsible Care®[11] program is an excellent example of governance in action for a market sector. Participation in Responsible Care is mandatory for all ACC member companies. This program

- measures and publicly reports performance through established environment, health, safet , and security measures
- is extending best practices to business partners through the industry supply chain
- reduced environmental releases by 80 percent over the past 17 years
- resulted in an employee safety record that is more than five times safer than the average of the U.S. manufacturing sector

The Responsible Care Security Code addresses facility, cyber, and transportation security. The Code requires ACC member companies to conduct comprehensive security vulnerability assessments, act on the results, and create security management systems. Implementing the code is mandatory. Additional guidance is available in their "Responsible Care Security Code of Management Practices" and *Implementation Guide for Responsible Care Security Code of Management Practices* [ACC 2002].

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.

The ACC is a member of the Chemical Sector Cyber Security Program, which states the following on its website:

> The Chemical Sector Cyber Security Program focuses on risk management and reduction to minimize the potential impact of cyber attacks on business and manufacturing systems.
>
> The Chemical Sector Cyber Security Program [ACC 2006] is structured to meet the common and unique needs of each segment and company type in the sector. Consistent with the Strategy, the Program is focused on five key initiatives for enhancing cyber security within the chemical sector:
>
> - Fostering involvement and commitment across the sector
> - Maintaining a robust cyber security public affairs program
> - Encouraging the adoption of established risk-based practices and guidance
> - Strengthening the industry's information sharing network
> - Encouraging the acceleration of improved security technology and solutions

Conclusion

Most senior executives and managers understand governance and their responsibilities with respect to it. The intent here is to help leaders expand their perspectives to include security and incorporate enterprise-wide security thinking into their own and their organizations' governance and management actions. An organization's ability to achieve and sustain adequate security starts with executive sponsorship and commitment.

---

1 Refer to the CERT Insider Threat website (http://www.cert.org/insider_threat) for presentations and podcasts on this subject.

2 See also [IIA 2000], [IIA 2001a], and [IIA 2001b].

3 Security as used here includes software security, information security, application security, cyber security, network security, and information assurance. It does not include disciplines typically considered within the domain of physical security such as facilities, executive protection, and criminal investigations.

4 The terms “organization” and “enterprise” are intended to convey the same meaning and are used interchangeably throughout the articles in this content area.

5 Convened after the National Cybersecurity Summit of 2004 [CGTF 2004].

6 http://www.entrust.com/news/index.php?s=43&item=249

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 2003].

8 The Organisation for Economic Co-operation and Development (OECD) also discusses the need to develop a “culture of security” in its Guidelines for the Security of Information Systems and Networks [OECD 2002] and in the companion implementation plan [OECD 2003].

9 See also “Characteristics of Effective Security Governance” for a table of eleven characteristics that compares and contrasts an organization with effective governance practices and one where these practices are missing [Allen 2007].

10 https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml

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

The Build Security In (BSI) portal is sponsored by the U.S. Department of Homeland Security (DHS), National Cyber Security Division. The Software Engineering Institute (SEI) develops and operates BSI. DHS funding supports the publishing of all site content.