Maturity of Practice

Julia H. Allen

November 2009

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

This article identifies several indicators that organizations are addressing security as a governance and management concern, at the enterprise level. It summarizes how some organizations, trade associations, and market sectors are proceeding. Many of the references and links in this article provide more detailed implementation guidance.

INTRODUCTION

Security's emergence as a governance and management concern is primarily taking place in the parts of the organization that provide and use IT. We currently see minimal attention paid to this topic during the early life cycle phases of software and system development, but increasing attention being paid during detailed design, coding, and testing.

However, as is the case for the entire Build Security In website, we believe that treating security as a governance and management concern, as a risk management concern, and as a project management concern at the earliest phases of the life cycle will produce more robust, less vulnerable software, resulting in a decline in the reactive, fire-fighting mode present in most IT and system operations and maintenance organizations.

INDICATORS OF PROGRESS

Consistent governance and management action across the organization is key. This includes attention and participation from business unit leaders, human resources, legal, audit, risk management, and finance, as well as IT and software

Software Engineering Institute
Carnegie Mellon University
4500 Fifth Avenue
Pittsburgh, PA 15213-2612

Phone: 412-268-5800
Toll-free: 1-888-201-4479

www.sei.cmu.edu

and system development groups.[1] Progress in executing some of these roles and actions is described in the following sections.

Protecting Information

One significant shift that is causing leaders to take note is the need to treat information, particularly consumer, customer, client, and employee information, with greater care, perhaps with the same care as money. Leaders understand the impact to their organizations' reputations if this is not done competently and breaches become public.[2] Customers expect that organizations will protect their privacy and their information and are becoming more aware of the risk of identity theft based on unintended data disclosure.[3] [PCI 2009a]. As stated on their website:

> *The PCI DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. This comprehensive standard is intended to help organizations proactively protect customer account data.*

The key requirements of DSS include the following:

1. Build and maintain a secure network.
2. Protect cardholder data.
3. Maintain a vulnerability management program.
4. Implement strong access control measures.
5. Regularly monitor and test networks.
6. Maintain an information security policy.

In addition, the PCI SSC has expanded their requirements for security with respect to payment applications in their Payment Application Data Security Standard [PCI 2009b] with the following requirements:

---

1 In his Ask the Auditor column titled "Who Is Responsible for Information Security? [Swanson 08]" Dan Swanson describes how leaders at all levels need to be involved to ensure adequate security.

2 Refer to the Privacy Rights ClearingHouse Website for a chronology of all publicly reported privacy breaches that have occurred since the ChoicePoint breach in 2005 (http://www.privacyrights.org/ar/ChronDataBreaches.htm).

3 http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm

1. Do not store sensitive authentication data after authorization (even if encrypted).
2. Protect stored cardholder data.
3. Provide secure authentication features.
4. Log payment application activity.
5. Develop secure payment applications (based on PCI DSS and industry best practices).
6. Protect wireless transmissions.
7. Test payment applications to address vulnerabilities.
8. Facilitate secure network implementation.
9. Never store cardholder data on a server connected to the Internet.
10. Facilitate secure remote software updates.
11. Facilitate secure remote access to payment applications.
12. Encrypt sensitive traffic over public networks.
13. Encrypt all non-console administrative access.
14. Maintain documentation and training programs.

Plan, Do, Check, Act describes how to integrate PCI DSS requirements with other accepted security standards for sustaining software security during deployment and operations.

Audit's Role

As part of the Critical Infrastructure Assurance Project, the Institute of Internal Auditors (IIA)[4] held six summit conferences in 2000 to better understand the role of governance with respect to information security management and assurance. They provided guidance in 2001 titled "Information Security Governance: What Directors Need to Know." This report includes case studies from General Motors, IBM, BellSouth, Intel, Sun Microsystems, the Federal Reserve Bank in Chicago, and Home Depot. Useful questions to ask that resulted from this work are listed in Efforts to Use as Exemplars below [IIA 2001a].

---

[4] "Established in 1941, The Institute of Internal Auditors (IIA) is an international professional association of more than 117,000 members. Throughout the world, The IIA is recognized as the internal audit profession's leader in certification, education, research, and technological guidance."

The Information Systems Audit and Control Association (ISACA)[5] and its partner organization, the IT Governance Institute (ITGI), have published extensive guidance on information technology and information security governance. Their report "Information Security Governance: Guidance for Boards of Directors and Executive Management" [ITGI 2006] addresses these questions:

1. What is information security governance?
2. Why is it important?
3. Who is responsible for it?

It also describes how to measure an organization's maturity level relative to information security governance.

ITGI describes these five basic outcomes of effective information security governance [ITGI 2006]:

1. Strategic alignment of information security with business strategy to support organizational objectives.
2. Risk management by executing appropriate measures to manage and mitigate risks and reduce potential impacts on information resources to an acceptable level.
3. Resource management by utilizing information security knowledge and infrastructure efficiently and effectively.
4. Performance measurement by measuring, monitoring, and reporting information security governance metrics to ensure that organizational objectives are achieved.
5. Value delivery by optimizing information security investments in support of organizational objectives.

Operational Resilience and Convergence

In its work with the Financial Services Technology Consortium (FSTC), Carnegie Mellon University's Software Engineering Institute is examining the convergence of security, business continuity, and IT operations management given their

---

[5] "ISACA is a leading information technology organization representing more than 50,000 individual members in more than 140 countries. Membership is comprised of all levels of IT professionals--executives, management and practitioners--all of whom are dedicated to the promotion of advanced IT governance, control and assurance practices."

critical impact on operational risk management.[6] The intent is "to improve the operational resiliency of the organization--the ability to adapt to a changing operational risk environment as necessary" [Caralli 2006]. In their technical reports Sustaining Operational Resilience: A Process Improvement Approach to Security Management [Caralli 2006] and Introducing the CERT Resiliency Engineering Framework: Improving the Security and Sustainability Processes [Caralli 2007], the authors offer an initial process improvement framework for operational resiliency and security. The framework has evolved into a structured management model that is highly influenced by the Software Engineering Institute's Capability Maturity Model Integration (CMMI).[7] It is being piloted with members of the FSTC, selected U.S. federal government agencies, and other collaboration partners [CERT 2009]. One process area in particular, titled Resiliency Technical Solution Engineering, describes goals and practices for addressing operational resiliency during software and system development.

A number of other organizations are beginning to describe their efforts to achieve organizational resilience through the integration of business continuity, operational and technology risk management, compliance, and information security and privacy, supported by audit. These integrating activities occur across products and business lines, and take into account people, business processes, infrastructure, applications, information, and facilities. Indicators of success include

- reduced risk of a business interruption
- shorter recovery time when an interruption occurs
- improved ability to sustain public confidence and meet customer expectations
- increased likelihood of complying with regulatory and internal service level requirements

The Alliance for Enterprise Security Risk ManagementSM is a coalition formed by ASIS International (representing the physical security community), ISACA, representing the IT audit community, and ISSA (Information Systems Security Association, representing the information security community). They are addressing "the integration of traditional and information security functions to encourage board and senior executive level attention to critical security-related

---

6 http://www.cert.org/resiliency

7 http://www.sei.cmu.edu/cmmi

issues" [AESRM 2005]. In their study "Convergence of Enterprise Security Organizations," the Alliance quotes the ASIS definition of convergence as follows:

> *The 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.*

They go on to describe five imperatives driving convergence[8] and the organizational implications with supporting examples. Additional white papers are available at the AESRM website.

These efforts are providing evidence of the value of addressing security as part of a broader convergence effort and in support of organizational preparedness.

A Legal View

The American Bar Association's Privacy & Computer Crime Committee has published a "Roadmap to an Enterprise Security Program" [Westby 2005]. The preface to the Roadmap states the following:

> *This publication was developed by a multidisciplinary team of industry representatives, government personnel, policy specialists, attorneys, technical experts, and academicians. They came together to provide a roadmap that links the various pieces of the cyber security "puzzle" into an orderly process that conforms with global standards and best practices, helps meet compliance requirements, facilitates cooperation with law enforcement, and promotes public-private sector cooperation.*

The Roadmap presents a structure that includes governance, security integration and security operations, implementation and evaluation, and capital planning and investment controls. The steps for governance include the following [Westby 2005]:

- Establish governance structure, exercise oversight, develop policies.
- Inventory digital assets (networks, applications, information).

---

[8] Rapid expansion of the enterprise ecosystem, value migration from the physical to information-based and intangible assets, new protective technologies blurring functional boundaries, new compliance and regulatory regimes, continuing pressure to reduce cost [AESRM 2005].

- Establish ownership of networks, applications, and information; designate security responsibilities for each.
- Determine compliance requirements with laws, regulations, guidance, standards, and agreements (privacy, security, and cybercrime).
- Conduct threat and risk assessments and security plan reviews (for internal and contractor operations). This may include certification and accreditation.
- Conduct risk management based on digital asset categorization and level of risk.

This view is further expanded into a detailed Governing for Enterprise Security Implementation Guide developed by Westby and Allen [Westby 2007].

A Software Engineering View

An emerging body of knowledge describes aspects of how to apply governance and management thinking to the engineering and development of secure software. In addition to John Steven's article Adopting an Enterprise Software Security Framework, there are other articles on the BSI web site that were previously published in a series in IEEE Security & Privacy. Adopting a Software Security Improvement Program provides several concrete steps and a progression of phases for improvement. Bridging the Gap between Software Development and Information Security describes a range of secure software development activities and practices to conduct during a software development life cycle.

Chapter 10 of Software Security: Building Security In [McGraw 2006] elaborates on several of the IEEE Security & Privacy articles. It describes elements of an enterprise software security program, addressing

- the business climate
- building blocks of change, including four common pitfalls:
  - over-reliance on late-life-cycle testing
  - management without measurement
  - training without assessment
  - lack of high-level commitment (particularly relevant for governance and management)
- building an improvement program
- establishing a metrics program, including a three-step enterprise rollout:
  - assess and plan
  - build and pilot
  - propagate and improve
- continuous improvement
- what about COTS (and existing software applications)?, including an enterprise information architecture

- adopting a secure development life cycle

Part I of The Security Development Lifecycle - SDL: A Process for Developing Demonstrably More Secure Software [Howard 2006] describes the need for a Secure Development Lifecycle (SDL). The authors, Michael Howard and Steve Lipner, state "The biggest single factor in the success of SDL is executive support." Effective commitment to an SDL includes making a statement, being visible, providing resources, and stopping the delivery of products that do not meet their security and SDL requirements. Part II describes the twelve-stage SDL.

Additional resources that provide in-depth descriptions of practices from governance to those recommended for addressing software security during all development and acquisition lifecycle phases include the following:

- Building Security In Maturity Model (BSIMM) v1.0
- Open Web Applications Security Project (OWASP) Software Assurance Maturity Model (SAMM) v1.0
- Microsoft's Security Development Life Cycle, Version 4.1
- Department of Homeland Security Assurance for CMMI Process Reference Model

CONCLUSION

The purpose of this article has been to demonstrate that many sectors, organizations, and organizational functions (including risk management, IT, business continuity, audit, legal, and software development) are making progress and producing results by treating security as an enterprise issue. They are taking governance and management actions to integrate security into ongoing business councils and steering groups, decision-making processes, plans, business and development processes, and measures of success.

Copyright © Carnegie Mellon University 2005-2012.

This material is based upon work funded and supported by Department of Homeland Security under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of Department of Homeland Security or the United States Department of Defense.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

This material has been approved for public release and unlimited distribution except as restricted below.

Internal use:* Permission to reproduce this material and to prepare derivative works from this material for internal use is granted, provided the copyright and "No Warranty" statements are included with all reproductions and derivative works.

External use:* This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other external and/or commercial use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

* These restrictions do not apply to U.S. government entities.

DM-0001120