Chapter 14
Integration of COBIT, Balanced Scorecard and SSE-CMM as an Organizational & Strategic Information Security Management (ISM) Framework

James E. Goldman
Purdue University, USA

Suchit Ahuja
Purdue University, USA

ABSTRACT

The purpose of this chapter is to present an integrated framework that addresses the need for organizational information security requirements as well as alignment between business, IT and information security strategies. This is achieved via the integrated use of control objectives for Information Technology (COBIT) and balanced scorecard (BSC) frameworks, in conjunction with Systems Security Engineering Capability Maturity Model (SSE-CMM) as a tool for performance measurement and evaluation, in order to ensure the adoption of a continuous improvement approach for successful sustainability. This integrated framework has been presented at the IEEE Symposium on Security & Privacy (2009) and the International Conference on Business/IT Alignment (2009). The goal is to investigate the strengths, implementation techniques, and potential benefits of such an integrated approach. The integrated use of COBIT, BSC, and SSE-CMM can provide a more comprehensive mechanism for strategic information security management–one that is fully aligned with business, IT, and information security strategies.

INTRODUCTION

Threats security of information assets and privacy of individuals have been growing at a tremendous rate. It is reported that more than 250 million records containing sensitive personal information were involved in security breaches in the U.S. since January 2005 (Privacy Rights Clearinghouse, 2009). In order to proactively deal with such growing threats to security and privacy of information-based assets, organizations are increasingly adopting information security man-

DOI: 10.4018/978-1-60960-573-5.ch014

agement systems (ISMS). Although organizations use several established international standards and frameworks like ISO27001, ISO 27799, ISO 27002, NIST, FIPS, ANSI, etc. for information security controls and management, the primary driving factor for such implementations are regulatory compliance requirements (Turner, Oltsik & McKnight, 2008). In order to be compliant with requirements of applicable industry regulations like Health Insurance Portability and Accountability Act (HIPAA), Sarbanes-Oxley (SOX), Gramm Leach Bliley Act (GLBA), Children's Online Privacy Protection Act (COPPA), Family Educational Rights and Privacy Act (FERPA), etc., organizations adopt ISMS and frameworks. The IT organization also adopts best practices and supporting tools like IT Infrastructure Library (ITIL), Control Objectives for Information Technology (COBIT), Capability Maturity Model Integration (CMMI), Six Sigma, etc. for IT service, support, quality management and information security management.

A standalone framework mostly addresses only a single functional area within the organization. Therefore, organizations often use a combination of frameworks to address the challenges of business, IT and operational information security. Nevertheless, integration of these frameworks and tools is not easy for organizations, as successful implementation is dependent on factors ranging from organizational culture to training of employees (Elci, Ors & Preneel, 2008). In the same way, organizations can gain additional value and benefits by using a combination of standards and best practices for strategic ISM. This view is also supported by studies that demonstrate a combination of standards such as ISO 17799 and SSE-CMM for metrics based security assessment (Goldman & Christie, 2004) and other studies that illustrate the mapping of processes for effective integration of COBIT and SEI-CMM (IT Governance Institute, 2007a). Several other studies also show that using a combination of standards and best practices can lead to effective management and alignment of IT with business.

Taking into account the above discussion, the goal of this chapter is to present an integrated framework that addresses the need for organizational information security requirements as well as alignment between business, IT and information security strategies. This is achieved via the integrated use of Control Objectives for Information Technology (COBIT) and Balanced Scorecard (BSC) frameworks, in conjunction with Systems Security Engineering Capability Maturity Model (SSE-CMM) as a tool for performance measurement and evaluation, in order to ensure the adoption of a continuous improvement approach for successful sustainability. The purpose is to investigate the strengths, implementation techniques, and potential benefits of such an integrated approach, while simultaneously aligning business, IT and information security strategies.

PROBLEM & SIGNIFICANCE

Lack of a Comprehensive Approach to Information Security

Organizations are increasingly using ISM frameworks in order to mitigate risks and reduce threats to business assets (mainly information assets). A purely technical approach to implementation of information security controls proves insufficient in addressing the strategic objectives of the organization. According to the results of a Global Information Security Survey (Ernst & Young, 2008), the primary drivers for investment and implementation of such ISM frameworks are regulatory compliance requirements, loss of revenue, loss of stakeholder confidence, loss to brand and reputation, etc. Thus, investments made by the organization (for technology alone) often provide low or inadequate returns, resulting in revenue losses and higher operational expenditures. It also establishes the fact that there is a gap