December 2007

Information Security Governance Arrangements: The Devil is in the Details

Srinivasan Rao
The University of Texas at San Antonio

Sriraman Ramachandran
The University of Texas at San Antonio

INFORMATION SECURITY GOVERNANCE ARRANGEMENTS: THE DEVIL IS IN THE DETAILS

SRINIVASAN RAO
Department of Information Systems and Technology Management,
The University of Texas at San Antonio
chino.rao@utsa.edu

SRIRAMAN RAMACHANDRAN
Department of Information Systems and Technology Management,
The University of Texas at San Antonio
sriraman.ramachandran@utsa.edu

Abstract

Information security governance includes the governance aspect, which sets the information security direction and strategy of an organization, and, the management aspect, which addresses how the strategy is implemented and managed. In this article, we focus on the management aspect of information security governance. Different organizational arrangements (i.e., governance arrangements) are possible to manage and implement the security strategy. One arrangement involves the creation of an information security department with a chief information security officer (CISO), or equivalent, to highlight the importance of security. Unfortunately, this may also create the impression that security is the responsibility of a special group and has little to do with the average employee. At the other extreme, no special security department is created. Instead, all employees have a significant role in maintaining information security in the organization. Such an arrangement may be more suited to implement guidelines, which suggest that security features are better built into business processes and software, rather than incorporated as an add-on layer. This arrangement diffuses the responsibility for security, and has the potential for diluting top management attention to security. In this research-in-progress paper, we propose a study to examine the effects of different governance arrangements.

Keywords

Information Security Governance, Chief Information Security Officer

Introduction

Corporate governance refers to the responsibilities of the Board of Directors and top management (von Solms, 2001a). Consistent with this definition, information security governance can be said to describe how information security is handled at the executive, (i.e., top management) level (Posthumus and von Solms, 2004). Posthumus and von Solms (2004) divide information security governance into governance aspects and management aspects. The governance aspects address how the Board of Directors and executive management "go about setting the information security direction and strategy of their organization." (Posthumus and von Solms, 2004; p. 644). The management aspects are concerned with "how an organization's security strategy will be implemented and managed." (Posthumus and von Solms, 2004; p. 644). The implementation and management of the security strategy requires the assignment of responsibilities for security functions among organizational personnel (IT Governance Institute, not dated). Several arrangements are possible. The arrangements used to assign responsibilities to manage and implement security strategy are referred to as governance arrangements. In this article, we briefly explore the effects of different governance arrangements, and propose a survey-based study to gather empirical evidence.

Researchers and practitioners have come up with loosely stated principles that may help an organization enhance information security. First, there is a call to top management to pay direct attention to issues related to security. Associated with this is the recommendation for the appointment of a chief information security officer (CISO). The guidelines are mixed on whether the CISO should report directly to the chief executive office (CEO) or to the chief information officer (CIO). A second principle that is stated is that security is better built into the business processes and business software applications, rather than layered onto existing processes and applications. This is consistent with the idea that security is the responsibility of all employees. Both principles have merit but may lead to conflicting secondary effects. For example, the establishment of a CISO may create the impression that primary responsibility for security is resident with that individual and his/her group, which is inconsistent with the principle that all employees have a responsibility for information security. Our goal is to tease out such inconsistencies based on the information in literature, and subsequently seek empirical evidence for the same.

The rest of the article is arranged as follows. In the next section, we briefly review the literature. Following that we discuss possible conflicts that could arise from the articulated guidelines. Lastly, we outline the survey that is currently under consideration.

Literature Review

In this section, we briefly examine two key bodies of literature. The first body relates to the calls for appointing a CISO, and the second body relates to the incorporation of security into organizational processes.

Calls for CISO

In a series of articles, von Solms and co-authors outline the roles and responsibilities of the Board of Directors/CEO (also referred to as executive management or top management) with respect to information security governance. The primary concept elucidated is that ".. information security governance is an essential part of corporate governance…" (von Solms and von Solms, 2004, p. 372), and that ".. the Board of Directors as well as the top management have a direct corporate governance responsibility towards ensuring that all the information assets of the company are secure, and that due care and due diligence have been taken to maintain such security." (von Solms and von Solms, 2004, p. 372). Such involvement in security is considered essential to demonstrate management's commitment to security. Further top management support is considered key to the success of an organization's security efforts (Posthumus and von Solms, 2004), which echoes an earlier statement by von Solms (2001) "Without this management support, information security managers fight a very difficult, and, often losing battle." (p. 216).

As a part of top management attention and control, it is often recommended that a CISO be appointed. For instance, an IT Governance Institute report recommends that the governance framework should include "an effective security organizational structure." (IT Governance Report, 2006, p. 18). It is recommended that as a part of the security organizational structure, the comprehensive security program includes "assignment of roles, responsibilities, authority and accountability." One part of the assignment of roles and responsibilities is the identification of information security leaders, who are held accountable, but provided with support. What is repeatedly emphasized is that an individual be "appointed to be responsible for developing, implementing and managing the information security program" (p. 34), with the implication that this person is the *de facto* CISO. It is further suggested that the CISO "should have sufficient authority and resources to accomplish security objectives."

In effect, practitioner organizations, such as the IT Governance Institute and the Institute of Internal Auditors imply that a CISO with a supporting group is essential to handle the managerial aspects of information security governance. The responsibilities expected of this group are that they will develop policies for functional groups to follow, develop initiatives to raise awareness, and monitor compliance.

Two arrangements are common. In our experience, we have noticed that some organizations create an information security group under the Information Technology (IT) group, with the CISO reporting to the Chief Executive Officer (CEO) through the Chief Information Officer (CIO). Other organizations create the information security group independent of the IT department, with the CISO reporting directly to the CEO. Other arrangements are discussed by Germain (2005).

Incorporation Of Security Into Business Processes

A second guideline that is often articulated is that security initiatives and processes need to be interwoven into business initiatives and processes. This is reflected in the following statement by IT Governance Institute: "Information security should be an integral part of enterprise governance and integrated into strategy, concept, design, implementation and operation." (p. 15).

The incorporation of security into business or the alignment of security with business can be viewed at three levels. First, at the strategic level, it is recommended that information security strategy be aligned with business strategy to support organizational objectives (IT Governance Institute, 2006). Second, the IT Governance Institute recommends, at the business process level, that "evaluating management processes from start to finish, along with their controls, can mitigate the tendency for the security gaps to exist amongst various functions." (p. 14). Further, it is recommended that "internal controls must be flexible and reviewed regularly." (Institute of Internal Auditors, not dated, p.6).

The third level addresses the incorporation of information security processes into the systems design process. Straub and Welke (1998) argue that "..planning for security should ideally be incorporated into systems development and security controls designed at the logical systems level in parallel with actual system functionality (Baskerville, 1993)" (p.450). A report from the Institute of Internal Auditors states, "You design security in from the beginning, you go through the testing, and you make sure you have validated that the application does what it is supposed to do, but not more that it is supposed to do." (p.17). However, this is not easy at a practical level. Tryfonas, Kiountouzis and Poulymenakou (2001) report "there is no pure methodological approach for the integration of the security requirements to the development processes, and wherever this does happen, it does so empirically, by exploiting previous experiences and basic features provided per situation."

In sum, the alignment of information security strategy with organizational strategy is a high level function that can be performed at the CISO level. However, the incorporation of security into the business processes and systems development are lower level processes, best performed by the functional groups and the IT development groups respectively. While a CISO or the security group may encourage such activity, it is the business units that are in a better position to assess what information is important and how much security is appropriate. Their willingness to examine the need for security steps and the incorporation of those steps are likely to be impeded if they view security as someone else's responsibility.

The Possible Conflict

We conceptualize three security governance arrangements: the security group as a separate entity, the security group as an entity within the IT group, and, no clearly defined security group (i.e., security responsibilities are diffused throughout the organization.)

Calls for the attention to security by executive management come from several beliefs. First, attention from executive management to any issue serves as a symbolic cue to the employees that that issue is important to the organization. Thus, the appointment of a CISO creates the perception among the employees that top management interest in security is high. Second, the appointment of a CISO clearly centralizes the responsibility for information security in the organization. The CISO is expected to develop initiatives that will enhance information security. Such initiatives include development of security policies, training, raising awareness, monitoring adherence to policies and so on. Third, the attention of top management to an area usually leads to access to resources to address problems in that area.

Other segments of the literature on security emphasizes that security is the responsibility of all employees. Such responsibility can be discharged in several ways. First, there is an expectation that all employees will adhere to organizational security policies and practices. Second, when business processes are designed/re-designed, the steps required to keep information secure will be incorporated into the processes, and not be ignored or included as a separate add-on step. Third, a corollary to the second issue is that security will be designed into the software application and not be ignored or added as a separate layer.

The issue that is of interest to us is – are the two guidelines discussed in conflict with each other, or, can they be managed to work together to strengthen information security in an organization? The argument that they may be in conflict with each other is as follows. The appointment of a CISO and the associated creation of a group to be responsible for security create the impression that the responsibility for information security rests with the CISO/security group. Consequently, individual employees do not see the importance of their own role in maintaining and enhancing information security, beyond compliance with policies coming down from the CISO's office. Such compliance may also be less than total, in particular, when it is seen to be in conflict with, or, is seen to hinder the core function of the employee.

The possibility that CISO office may be consistent with increasing employee participation in increasing information security may be argued as follows. The CISO office implements initiatives such as policies and training. These increase employee awareness of their role in maintaining information security, and consequently may promote security-related behaviors, including building in security processes into business processes.

In our anecdotal experience, we have observed a tendency on the part of employees to absolve themselves of the security-related responsibilities, when a security-related office is created. On the other hand, in literature, there is no explicit connection made between the appointment of a CISO and individual employee behaviors, but there appears to be an implicit belief that the CISO can, through policy formulation, training and awareness, affect employee security behaviors throughout the organization. However, the implicit beliefs in literature still lack empirical support.

The purpose of our research is to empirically test our anecdotal observations against the expectations of those making recommendations regarding governance.

Proposed Study

The independent variable in the study will be governance arrangement. The governance arrangement factor will be a categorical variable, and, will have one of three values: no special security department, special security department under the umbrella of the IT department, and, an independent security department.

The dependent variables will be the following: the extent of access to top management on security-related issues, the extent to which security is built into business processes/systems development, and employee perception of top management interest in security.

The study will be conducted at an organizational level. Two key groups of respondents will be surveyed in each organization. One (or two high level) manager(s) will be surveyed to gather information on the governance arrangement and the extent of access to the top management on security-related issues. The second key group of respondents will include a few individuals from a functional department, and a few individuals from the information technology department. Functional group members will be queried on the extent to which security is incorporated into business processes, and also on their perception of top management interest in security issues. Respondents from the IT department will be queried on the extent to which security issues are built into the systems development process and also on their perception of top management interest in security-related issues.

Organizational demographic factors such as organizational size and industry type will also be recorded. The effect of these on the governance arrangement will be examined.

References

Baskerville, R.(1993). An analytical survey of information systems security design methods: Implications for information systems development, *ACM Computing Surveys,* **25**(4), p. 375-414.

Germain, J.M. (2005). Your next job title: CISO? http://www.cio.today.com/story.xhtml?story_id=0320013PMOQO&page=1 (last viewed Apr 29, 2007).

Institute of Internal Auditors (date). Information security governance: What directors need to know. http://www.theiia.org/download.cfm?file=7382 (last viewed Mar 5, 2007)

IT Governance Institute (2006). Information security governance: Guidance for Board of Directors and executive management (2nd Edition), http://www.itgi.org/template_ITGI.cfm?template=/ContentManagement/ContentDisplay.cfm&ContentID=6672 (last viewed Mar 5, 2006).

Posthumus, S. and von Solms, R. (2004). A framework for the governance of information security. *Computers and Security,* **23**, p. 638-646.

Straub, D.W. and Welke, R.J. (1998). Coping with systems risk: Security planning models for management decision making, *MIS Quarterly,* Dec 1998, p. 441-469.

Von Solms, B. (2001a) Information security – A multidimensional discipline, *Computers and Security,* **20**, p. 504-508.

Von Solms, B. and von Solms, R. (2004) The 10 deadly sins of information security management, *Computers and Security,* **23,** p. 371-376.