Chapter 3

Governing Information Security: Governance Domains and Decision Rights Allocation Patterns

Yu “Andy” Wu
University of North Texas, USA

Carol Saunders
University of Central Florida, USA

ABSTRACT

Governance of the information security function is critical to effective security. In this paper, the authors present a conceptual model for security governance from the perspective of decision rights allocation. Based on Da Veiga and Eloff’s (2007) framework for security governance and two high-level information security documents published by the National Institute of Standards and Technology (NIST), the authors present seven domains of information security governance. For each of the governance domains, they propose a main decision type, using the taxonomy of information technology decisions defined by Weill and Ross (2004). This framework recommends the selection of decision rights allocation patterns that are proper to those decision types to ensure good security decisions. As a result, a balance can be achieved between decisional authority and responsibility for information security.

INTRODUCTION

Increasingly, the advantages of information technology (IT) governance are being recognized. Good IT governance can promote empowerment and control of IT professionals. Decision making authority as an area of IT governance has been examined by some researchers (e.g., Grover, Henry, & Thatcher, 2007; Weill, 2004; Weill & Ross, 2004). However, more scrutiny is needed of the extension of governance concepts to information security. For instance, Grover et al. (2007) do not specifically address security and Weill and Ross (2004) treat “security and risk” simply as a cluster in “IT infrastructure services.” This classification reflects the traditional view of information security as a mere technical issue. Fresh considerations of information security call for a more fine-grained treatment of governance of security decisions. In particular, while some decisions have a clear tech-
nology orientation, others must address strategic, business-oriented goals. Still others lie somewhere in between. None can be ignored.

To aid the study and practice of information security governance, we propose a conceptual governance framework (Figure 1). It specifically deals with security decision rights and is based on the synthesis of a number of relevant concepts, principles, and taxonomies: (1) The concept of “structures of responsibilities” in information security (Backhouse & Dhillon, 1996); (2) The principle of harmonizing responsibility (accountability) with commensurate decision authority (Grover et al., 2007); (3) The principle of giving decision authority to the organizational unit with the best information for the decision (Galbraith, 1973, 1993; Simon, 1960); (4) A taxonomy of IT decision types (Weill, 2004; Weill & Ross, 2004); (5) A taxonomy of key domains in information security derived from Da Veiga and Eloff (2007) and two high-level information security documents published by the National Institute of Standards and Technology (NIST), SP 800-35 and SP 800-100; and (6) The tested practice of applying patterns to recurrent problems (Schumacher, Fernandez-Buglioni, Hybertson, Buschmann, & Sommerlad, 2006; Weill, 2004; Weill & Ross, 2004).

In the following sections, we elaborate on each of these as we build our information security governance framework. Tables 1 and 2 summarize its major components.

Our framework contributes to the IT governance literature by moving from Weill and Ross’ (2004) single-facet decision subtype of “security and risk” to a broader range of decision types involved in information security. For the information security literature, our framework connects a now well-established taxonomy of IT decision

---

**Table 1. Weill and Ross (2004) Governance archetypes**

<table>
<thead>
<tr>
<th>Archetype</th>
<th>Decision Rights Allocation Mechanisms</th>
<th>Interaction Pattern Between Business Management and IT Departments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business monarchy</td>
<td>Senior business executives make IT decisions for the entire enterprise. The IT executive is considered as one voice in the decision making.</td>
<td>Business executives make decisions about IT. The enterprise IT head, the CIO, is an equal partner with other executives.</td>
</tr>
<tr>
<td>IT monarchy</td>
<td>IT professionals make the IT decisions.</td>
<td>IT monarchy may be implemented in different flavors, involving IT professionals at enterprise IT function or business unit IT function to variable degrees.</td>
</tr>
<tr>
<td>Feudal</td>
<td>Business unit management makes IT decisions.</td>
<td>IT function may implement these decisions at the enterprise or business unit level.</td>
</tr>
<tr>
<td>Federal</td>
<td>Both the enterprise and business unit leaders are involved in making IT decisions.</td>
<td>Either enterprise IT function or business unit IT function or both can be involved in decision making.</td>
</tr>
<tr>
<td>IT duopoly</td>
<td>Decisions are made by the duo of IT executives and either enterprise business executives or business unit leaders.</td>
<td>This archetype also incarnate in one of these two forms: (a) “Bicycle wheel” with the enterprise IT function sitting at the hub. Sitting at the rim are the business units, each of which forms a spoke together with the hub; or (b) “T” arrangement, with the enterprise IT head having overlapping memberships in an executive committee and an IT committee.</td>
</tr>
<tr>
<td>Anarchy</td>
<td>No IT governance.</td>
<td></td>
</tr>
</tbody>
</table>
Related Content

An Integrated Framework for Strategic Information Systems Planning and Development
www.igi-global.com/article/integrated-framework-strategic-information-systems/51061?camid=4v1a

Context-Aware Framework for ERP
www.igi-global.com/chapter/context-aware-framework-erp/13662?camid=4v1a

A Language/Action Based Approach to Information Modelling
www.igi-global.com/chapter/language-action-based-approach-information/13916?camid=4v1a

E
www.igi-global.com/chapter/119566?camid=4v1a