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-
Technology 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 types.
Related Content

Autopoietic Approach for Information System and Knowledge Management System Development
[www.irma-international.org/chapter/autopoietic-approach-information-system-knowledge/13590/](www.irma-international.org/chapter/autopoietic-approach-information-system-knowledge/13590/)

A Fast and Space-Economical Algorithm for the Tree Inclusion Problem
[www.irma-international.org/chapter/a-fast-and-space-economical-algorithm-for-the-tree-inclusion-problem/215930/](www.irma-international.org/chapter/a-fast-and-space-economical-algorithm-for-the-tree-inclusion-problem/215930/)

A Texture Segmentation Algorithm and Its Application to Target Recognition

A Descriptive Model for End-User Acceptance of Information Centers
[www.irma-international.org/article/descriptive-model-end-user-acceptance/50952/](www.irma-international.org/article/descriptive-model-end-user-acceptance/50952/)

The 3-D Model of Information Systems Success: The Search for the Dependent Variable Continues
[www.irma-international.org/article/model-information-systems-success/51027/](www.irma-international.org/article/model-information-systems-success/51027/)