**Association for Information Systems**
**AIS Electronic Library (AISeL)**

AMCIS 2005 Proceedings

Americas Conference on Information Systems (AMCIS)

2005

# Information Systems Security and Information Systems Structure: A Contingency Perspective

Kregg Aytes
*Idaho State University*, aytekreg@isu.edu

Nicholas L. Ball
*University of Minnesota*, nball@csom.umn.edu

# Information Systems Security and Information Systems Structure: A Contingency Perspective

**Kregg Aytes**
Idaho State University
aytekreg@isu.edu

**Nicholas L Ball**
University of Minnesota
nball@csom.umn.edu

**ABSTRACT**

Although there are several general prescriptions for managers to follow in developing an information security system, these recommendations typically assume a relatively centralized, homogeneous organization with a culture that is conducive to compliance with documented rules and procedures. This paper describes a research project that is intended to understand how the IS functional structure affects the development and implementation of an information security system. Commonly-used guides, for developing an information security system, along with their imbedded assumptions about organizational structure are discussed. Elements comprising the IS functional structure are introduced, followed by discussion of the potential relationships among these elements and the elements of an information security system. Finally, a research project is described that will lead to a better understanding of these relationships.

**Keywords**

Information Systems Security, Information Systems Structure, Security Effectiveness

## INTRODUCTION

Information security has become an important aspect of IT management in recent years. One place that managers can look for guidance is to the various security frameworks and "best practices" guidelines available through a number of organizations. At this time, there is no lack of general prescriptions for how an organization should secure its systems. What may be lacking, however, is a way for management to understand how best to apply these recommendations to the various complex organizational arrangements that exist in most modern firms.

## INFORMATION SECURITY SYSTEM

An information security system, for the purposes of this paper, consists of four related components: Security policies, security standards, security procedures, and security practices. These first three components are listed in increasing level of detail, each level describing more specifically how the organization should deal with security issues. The last component, security practices, is concerned with how members of the organization actually behave with regards to information security.

Policies define the major security issues for the organization, describing general courses of action. For example, to reduce the threat of email-borne viruses, the organization may have a policy that no executable files will be sent or received via email. A security standard defines in more detail how this is to be done. Continuing with the previous example, the organization may set a security standard that all executable files will be blocked by the mail server. A security procedure defines the technology and/or process that will implement the security standards. The security procedure in this example would be to implement a setting on the mail server to block all emails containing attachments with certain executable file types. Finally, the security practice is concerned with how members of the organization, including users and IT staff, comply with the security procedures. For example, users in the organization, as a way of being able to receive executable files via email, may setup mail accounts with other providers (e.g., Hotmail) and then receive mail from that email provider while at work and thereby not actually comply with the security policy. An effective information security system ultimately depends on the actions of its organizational members.

## SECURITY MANAGEMENT MODELS

Security models provide guidance to the development of an information security system. Two widely-used security models were developed by the U.S. National Institute of Standards and Technology (NIST) and the International Organization for Standardization (ISO). The NIST model, which is an approach described in a series of "special publications" (available at

http://csrc.nist.gov/publications/nistpubs/index.html), is used as a guide within the U.S. federal government and other agencies.

Another widely-used model is the ISO 17799 model. This model is associated with an internationally-recognized certification provided to organizations that meet the standards presented in the model. This model is widely referenced in Europe, where ISO certification is an important factor in many business relationships.

Other recommendations and guidelines are available from CERT and IETF, as well as from a multitude of security consultants and hardware and software vendors. A common feature of many of these guidelines and models is the recommendation that a security policy or plan include identifying and assessing information assets and risks to those assets, determining appropriate controls (both technical and operational), implementing those controls, and auditing compliance after implementation. A further assumption is that the results of all the above be formally documented.

Imbedded in these recommendations, then, are assumptions about the way the firm is organized and functions. It appears that these guidelines and models would best fit organizations that are relatively centralized, do not contain too many disparate organizational units and systems, and have a culture conducive to compliance with formal policies and procedures. However, this is not the case for many contemporary firms. Is it possible to have other organizational configurations and still have effective information security systems? A question similar to this was posed as part of an industry survey in 2002. Information Security magazine conducted a survey of firms of all different sizes, and asked about their information security efforts (Briney and Prince, 2002). There were significant differences in how small and large organizations used security policies and allocated resources to security efforts. While the results of this survey make it difficult to determine the precise factors that influence security efforts, there appears to be a relationship with the centralization and complexity of the organization.

## ENTERPRISE-LEVEL INFORMATION SYSTEMS STRUCTURE AND THE STRUCTURE OF IS SECURITY

There is a substantial body of research on IS structure, divided into two large categories: that which describes the technological elements of IS structure and that which describes the organizational elements of IS structure. Literature related to the technological elements of IS structure has highlighted range and reach (Keen, 1991; Broadbent and Weill, 1997), standardization (Ross, 2003), and centrality (Fiedler, et al., 1996; Ahituv, et al., 1989; Leifer, 1988; Ein-Dor and Segev, 1982) of organizational systems as key technological structure constructs.

Range refers to the breadth of IS services that can be delivered across the organization. Reach describes the pervasiveness of these services across the organization. Range and reach taken together comprise two main aspects of technological complexity[1]. IS standardization refers to organizational specifications which limit the number of different technologies, data, processes, and systems utilized in the organization. The level of centrality refers to the geographic concentration of processing and storage of enterprise data.

A significant body of IS structure research has examined organizational elements of structure (Sambamurthy and Zmud, 1999; Brown and Bostrom, 1994; Brown, 1997; Olson and Chervany, 1980). Much of this literature has focused on locus of control of IS decisions. This focus on locus of control has led to research that has identified structural modes for organizing the IS function (for example centralized, decentralized, and federal organizations as described by Sambamurthy and Zmud, 1999). However, this research has not been particularly effective for describing more than high-level differences between firms. Given that most organizations are federal organizations (Sambamurthy and Zmud, 1999), utilizing this framework for describing differences firms' security management practices is unlikely to yield much promise.

The organizational theory literature has outlined three important constructs for describing structure: complexity/ differentiation, formalization, and centralization (Pugh, et al., 1968; Reimann, 1974). The literature describes four types of complexity/differentiation (Damanpour, 1996; Blau, 1970; Mileti, et al., 1977): occupational, spatial, vertical, and horizontal. Occupational differentiation refers to the number of different job titles that exist in the firm. Spatial differentiation describes the extent of geographically different locations in the firm. Vertical differentiation refers to the number of different hierarchical levels in the organization. Horizontal differentiation refers to the number of different organizational subunits that report to the chief executive officer. Formalization refers to the extent to which written rules and procedures specify the roles and interactions of organizational members. Finally, centralization refers to the organizational level where decision-making occurs.

[1] In much the same way that the project complexity literature highlights the number of elements and interactions among those elements as key components of project complexity (William, 1999; Baccarini, 1996; Wood, 1986).

Each of these organizational structure variables can be applied to the IS function (Brown and Bostrom, 1994). IS complexity or differentiation would refer to the extent to which there are many different job titles or organizational specialties in the IS function, the number of different hierarchical levels on the IS organization, the number of different sub-organizational units which report to the chief information officer, and the number of geographically distinct sites that must be managed by the IS organization. Formality would describe the extent to which written rules and procedures define organizational roles and activities. Centralization would include both the level at which IS decisions are made and whether these decisions are made by business executives or IS executives.

A further examination of the organizational theory literature highlights the relationships among these variables. Although there is some disagreement concerning the dimensionality of the structure construct, there is general consensus that complexity is positively related to formality and both are negatively related to centralization. One interpretation of this is as the complexity of the organization increases it becomes more difficult to maintain control through centralization. Instead, control is exercised by empowering employees to make decisions, but formalizing or specifying how those decisions are to be made.

Consistent with our discussion of enterprise-level IS structure, we conceptualize the structuring of IS security policies, standards, procedures, and practices in terms of formality of IS security policies and standards and centralization of procedures and practices.

## PRELIMINARY RESEARCH MODEL AND SAMPLE PROPOSITIONS

The theoretical underpinning of this research has its roots in the structural contingency theory, which presents the argument that the appropriateness of an organizational structure is contingent on organizational and environmental characteristics. Although one might imagine many relevant contingencies[2], we examine the effect of various enterprise-level IS structure variables on the structuring of IS security policies, standards, procedures, and practices. Utilizing structural contingency theory as a lens, we develop propositions that highlight enterprise-level IS structure constructs as important determinants of IS security structure.

A preliminary research model is presented below (see Figure 1). We theorize that enterprise-level IS structure variables impact the structuring of IS security policies, standards, procedures, and practices either directly or as modifiers of the relationship between how IS security is structured and the effectiveness of IS security system. Sample research propositions that will be examined include:

- Technical complexity is positively related to the degree of formalization of information security policies and standards.
- Technical complexity is negatively related to the degree of centralization of information security procedures and practices.
- Organizational complexity is positively related to the degree of formalization of information security policies and standards.
- Organizational complexity is negatively related to the degree of centralization of information security procedures and practices.
- The extent of organizational information security education is positively related to the degree of formalization of information security policies and standards.
- The extent of organizational information security education is negatively related to the degree of centralization of information security procedures and practices.

The relationships among the constructs specified in the research model will be examined in stages. During the first stage, the relationships among complexity, formalization of security policies and standards, centralization of procedures and practices, and information security education will be examined. In the second stage, the relationships among formalization of security policies and standards, centralization of procedures and practices, information security education, and the effectiveness of the security system will be assessed. Additionally, the moderating effects of organizational formalization, technical standardization, organizational centralization, and technical centrality will be examined in stage two.

[2] For example Sambamurthy and Zmud (1999) highlight several contingencies which impact locus of control.

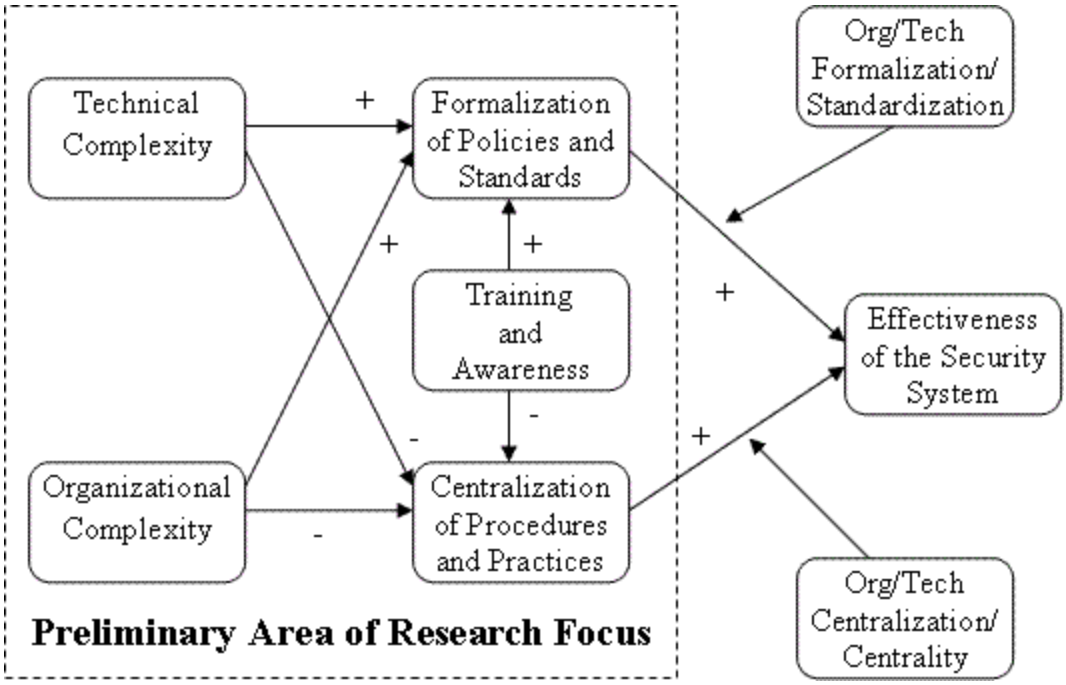


Figure 1 – Preliminary Research Model

## METHODOLOGY

The research presented in this paper is exploratory in nature. We will first concentrate on the antecedents of the effectiveness of the security system: technical and organizational complexity, formalization, and centralization. Frameworks for conceptualizing the security constructs presented in this paper and metrics for operationalizing the underlying variables are in the process of being formalized. The development of such metrics and frameworks will require a three-stage research project. During the first stage, conceptual frameworks will be developed along with specific hypotheses. Building upon a foundation of the current literature in this area, interviews will be conducted with both senior IS executives and those charged with information security. Stage two will be comprised of efforts to develop and validate measurement instruments to operationalize the key security management variables. Such instruments will be developed following the process prescribed by Churchill (1979) and will be greatly aided by interactions with the executives described above. Finally, the hypotheses will be examined in stage three. It is anticipated that the hypotheses will be tested with data gathered from a survey of large corporations in the United States.

## REFERENCES

1. Ahituv, N., Neumann, S., & Zviran, M. (1989). Factors affecting the policy for distributing computing resources. *MIS Quarterly, 13*(4), 388.
2. Baccarini, D. (1996). The concept of project complexity - a review. *International Journal of Project Management, 14*(4), 201-204.
3. Blau, P. M. (1970). A formal theory of differentiation in organizations. *American Sociological Review, 35*(2), 201-218.
4. Briney, A. & Prince, F. (2002). Does Size Matter? *Information Security*, September, 36-39.
5. Broadbent, M., & Weill, P. (1997). Management by maxim: How business and IT managers can create IT infrastructures. *Sloan Management Review, 38*(3), 77.
6. Brown, C. V. (1997). Examining the emergence of hybrid IS governance solutions: Evidence from a single case site. *Information Systems Research, 8*(1), 69.

7. Brown, C. V., & Bostrom, R. P. (1994). Organization designs for the management of end-user computing: Reexamining the contingencies. *Journal of Management Information Systems, 10*(4), 183.
8. Churchill Jr., G. A. (1979). A paradigm for developing better measures of marketing constructs. *Journal of Marketing Research (JMR), 16*(1), 64.
9. Damanpour, F. (1996). Organizational complexity and innovation: Developing and testing multiple contingency models. *Management Science, 42*(5), 693.
10. Ein-Dor, P., & Segev, E. (1982). Organizational context and MIS structure: Some empirical evidence. *MIS Quarterly, 6*(3), 55.
11. Fiedler, K. D., & Grover, V. (1996). An empirically derived taxonomy of information technology structure and its relationship to.. *Journal of Management Information Systems, 13*(1), 9.
12. Keen, P. (1991). *Shaping the future: Business design through information technology*. Boston, MA: Harvard Business School Press.
13. Leifer, R. (1988). Matching computer-based information systems with organizational structures. *MIS Quarterly, 12*(1), 62.
14. Mileti, D. S. 1., Gillespie, D. F. 2., & Haas, J. E. 3. (1977). Size and structure in complex organizations. *Social Forces, 56*(1), 208.
15. Olson, M. H., & Chervany, N. L. (1980). The relationship between organizational characteristics and the structure of the information services function. *MIS Quarterly, 4*(2), 57.
16. Pugh, S. 1., Hickson, D. J. 1., Hinings, C. R. 2., & Turner, C. 3. (1968). Dimensions of organization structure. *Administrative Science Quarterly, 13*(1), 65.
17. Reimann, B. C. (1974). Dimensions of structure in effective organizations: Some empirical evidence. *Academy of Management Journal, 17*(4), 693.
18. Ross, J. W. (2003). Creating a stratgic architecture competency: Learning in stages. *MIS Quarterly Executive, 2*(1), 31-43.
19. Sambamurthy, V., & Zmud, R. W. (1999). Arrangements for information technology governance: A theory of multiple contingencies. *MIS Quarterly, 23*(2), 261.
20. Williams, T. M. (1999). The need for new paradigms for complex projects. *International Journal of Project Management, 17*(5), 269.
21. Wood, R. E. (1986). Task complexity: Definition of the construct. *Organizational Behavior & Human Decision Processes, 37*(1), 60.