2005

Decision Making, IT Governance, and Information Systems Security

Yu Andy Wu
University of Central Florida, ywu@bus.ucf.edu

Carol S. Saunders
University of Central Florida, csaunders@bus.ucf.edu

Decision Making, IT Governance, and Information Systems Security

Yu “Andy” Wu
University of Central Florida
ywu@bus.ucf.edu

Carol S. Saunders
University of Central Florida
csaunders@bus.ucf.edu

ABSTRACT

The complex issue of IS security involves organizational factors. Decision making, an important area of organizations, however, has only been studied to a limited extent in relation to IS security. In this paper we explore the relationship between organizational distribution of decision rights and IS security. We review the security literature and identify three aspects of an organization as what we term the pillars bolstering the success of IS security – people, processes/structures, and technology. We top our IS Security Architecture with the integrative truss of IS security strategy. Employing Weill and Ross’ (2004) IT governance archetypes, we link this IS Security Architecture to IT governance, and propose that IT governance patterns can enhance security when the governance archetype in place matches the decision profile required by a security practice.

KEYWORDS

IS Security, organizational decision making, decision rights, IT governance.

The anatomy of the organization is to be found in the distribution and allocation of decision-making functions.

- Herbert Simon

INTRODUCTION

With their increasing reliance on information technology, organizations face the ever more challenging job of safeguarding their information systems and information stored therein. Although they are gaining some grounds (BSA and ISSA, 2003), surveys still find security breaches commonplace (e.g., CSI and FBI, 2002) , financial loss sizable (e.g., Whitman, 2003), and risk still imminent for many organizations (e.g., BSA and ISSA, 2003). Consequently, “security and privacy” has risen to the third spot, its highest ever, in IT executives’ list of top five management concerns in the SIM survey (Luftman and McLean, 2004).

IS security is a complex issue involving not merely technical but also organizational factors (Dhillon and Backhouse, 2000). Decision making is an organizational factor that interests many organizational design researchers. However, IS security decision making has not been studied in much depth.

We, therefore, explore how an organization’s distribution of decision rights influences its IS security. First, we review the security literature and identify three important organizational aspects that we describe as “pillars” to bolster IS security success. IS security strategy offers the overarching integrative mechanism in our IS Security Architecture. Each of these architectural component is operationalized by a related “key security practice,” which by itself involves numerous decisions. Organizational decision making can be enhanced by the use of lateral organizations, “a mechanism for decentralizing general management decisions” (Galbraith, 1993, p. 6). Since lateral organizations make it possible for decisions to be made by the people most familiar with the decision and its implications, they are becoming increasingly prevalent in today’s uncertain, dynamic world. Lateral organizations also facilitate essential activities for IS security effectiveness and serve as the building blocks of IT governance. Specifically to examine lateral organizations in the IT context, we employ Weill and Ross’ (2004) IT governance archetypes. We propose that the match between the governance archetypes in place and the required decision profiles is important.

THE ARCHITECTURE OF IS SECURITY

We reviewed relevant academic IS literature to identify the important enablers of successful IS security. Similar to the results of Dhillon and Backhouse’s (2001) extensive effort to chart the territory, we found few security studies and frameworks, although researchers are beginning to examine the impacts of organizational factors, such as size, industry type, top management support, etc. (e.g., Kankanhalli, Teo, Tan and Wei, 2003; Kotulic and Clark, 2003).

To broaden our scope, we drew from two additional literature sources: practitioner literature and survey reports. Some practitioner literature authors have gone beyond the technical and “checklist” (Dhillon and Backhouse, 2001) approach and examined security from an organizational angle (e.g., Purser, 2004; Wylder, 2004). Their insights provide inspiration for more strenuous academic research. The various surveys conducted by security organizations (e.g., Brainbench and ITAA, 2003; BSA and ISSA, 2003), government agencies (CSI and FBI, 2004), and accounting firms (e.g., Ernst & Young LLP, 2004) also furnish insightful analyses, as well as data and statistics that may help researchers identify interesting questions.

These three sources of literature, intriguingly, converge on important security issues. They identify three major aspects that are critical to IS security: people, processes/structures, and technology. Table 1 lists the terms the various studies use to describe each aspect. Although the terminology varies, they clearly identify the same aspects of organizational life. We call these aspects the “pillars” of IS security.

Study	**Dhillon (2001a)**	**Dhillon (2001b)**	**Whitman (2004)**	**Boyce and Jennings (2002)**	**Ernst & Young (2004)**
Type	Academic	Academic	Academic, Survey*	Practitioner	Survey
People	Behavioral practices (human issues, culture, normative controls)	Pragmatic aspects**	Education, training, and awareness programs	People	People
Structures/ Processes	Formalized rule structures	Formal rule base aspects	Policy	Operation	Processes
Technology	Technological controls	Technical systems	Security mechanisms/controls	Technology	Technology

* Whitman’s analyses are based on both empirical data in his academic studies and third-party survey results.
** Dhillon calls this “pragmatic aspects.” However, based on his discussion of the principles for this aspect, it is in fact a human aspect.

Table 1. Key Organizational Aspects (Pillars) of IS Security

Whitman (2004) does not use a high level terminology to identify the areas. However, he insightfully concludes that security should be addressed through (a) policy, (b) security mechanisms/controls, and (c) education, training, and awareness programs. These elements coincide with what we, in our subsequent discussion, will use to operationalize the three pillars. We operationalize the people pillar as “Awareness Programs,” which are instrumental for building a security-aware culture. Although culture transcends awareness programs (Dhillon, 2001), the latter is easier to measure empirically. For the structures/processes pillar, written policies, especially the top level policy, set the tone of the organization’s security practices. Therefore we examine this pillar from the angle of “Top-Level Policy.” “Security Defense Mechanisms” reflect the technology pillar. Hereinafter, we refer to these security practices for operationalizing the pillars as “key (security) practices.”

To successfully integrate these three pillars, moreover, an organization needs a security strategy, which is a roadmap defining its desired status of security and intended course of action to reach that status (Purser 2004). Dhillon (2001) states that a security vision and strategy ensures that IS security will lead to an integral business environment. Wylder (2004) goes as far as arguing that IS security strategy should be part of an organization’s strategic plan. Thus, an integrative strategy is the “truss” that integrates the three pillars to support security success. IS security strategy judiciously distributes the onus (decision responsibilities, centers, etc.) depending upon environmental and organizational factors such that the most effective and harmonious combinations are exploited. The three pillars can accommodate incremental strategy shifts. However when substantive changes that redefine the capabilities and constituents are needed, it is the integrative IS security strategy that must be modified.

IS SECURITY AND LATERAL ORGANIZATIONS

Each of the three pillars of IS security has a key practice and involves important decisions. Table 2 lists some examples. "When an organization makes decisions using a developed security mind, it separates itself from the struggle and costs commonly associated with information security" (Day 2003, p. 284).

Security Pillar/Truss	Key Practice	Definition of Key Practice	Example of Decisions
Integrative Strategy	IS Security Strategy	An organization's roadmap defining its desired status of security and intended course of action to reach that status (Purser, 2004).	Which of the three security strategies to deploy: security by obscurity, perimeter defense, or defense in depth (Boyce and Jennings, 2002).
People	Awareness Program	The mechanism to ensure that the organization's security posture is well understood and reflected by the organizational culture (Purser, 2004).	Decisions for identifying current training needs, segmenting the user community, employing effective media and presentation formats, and designing the training around the users' work patterns (Boyce and Jennings, 2002; Peltier, 2002).
Processes/ Structures	Top-Level Policy	"A high-level statement of organizational beliefs, goals, and objectives and the general means for their attainment as related to the protection of organizational assets" (Peltier, 2002, p. 22).	What constitutes important information for the organization and thus should be controlled; who should be developing the policies (Boyce and Jennings, 2002; Peltier, 2002).
Technology	Security Defense Mechanisms	An organization's IT infrastructure, hardware, software, etc. that combined form a system of security measures that will effectively thwart the attackers (Clark, 2003).	Choice of filtering measures, placement of firewall, and servers to install when configuring the "demilitarized zone" (DMZ) between the public Internet and the organization's intranet (Clark, 2003; Day, 2003).

Table 2. IS Security Architecture Components, Key Practices, and Decision Making

A decision in good hands is more likely to be a good decision. How decision rights are distributed is a function of the human traits, tools, and the task environment (Simon, 1960). Mulder (1960) succinctly defines decision structure as "who makes decisions for whom (p. 2)" and suggests that it is independent of the formal hierarchy. He shows that decision structure, not topology, determines group performance. Although Mulder argues for a centralized decision structure, Galbraith (1993) is an ardent proponent of decentralization through lateral organizations, which are "microcosm" that brings expertise and perspectives from various functions to work on a given decision. Lateral organizations cut across the vertical hierarchy and enable an organization to make more and better decisions (Galbraith, 1973, 1993). As with what they do for other decisions, lateral organizations also enhance decision making in IS security. This is achieved in three ways.

First, lateral organizations facilitate information processing hence uncertainty reduction. The only certainty about IS security is that absolute certainty and security is impossible (Boyce and Jennings, 2002; State of Colorado, 2003). Organizations must have the necessary information processing capacity to reduce uncertainties to an acceptable level (Boyce and Jennings, 2002). When task uncertainty increases, the number of exceptions also increases and may overload the organizational hierarchy if only vertical communication channels are followed. By bringing decisions to where the first-hand information is available, lateral organizations increase organizations' information processing capability (Galbraith, 1993).

Second, lateral organizations facilitate the identification of structures of responsibility. A vehicle to ensure prompt actions is the "structures of responsibility" (Backhouse and Dhillon 1996), which serve to identify the responsible agents and their underlying patterns of behavior. Lateral organizations create additional communication channels not present in the vertical hierarchy (Joyce, McGee and Slocum, 1997), which help the organization better understand the informal norms, the juxtaposition of formal and informal security management structures, and the attribution of blame, responsibility, accountability, and authority. All of these, according to Backhouse and Dhillon (1996), are conducive to establishment of security baseline and trigger points.

Third, lateral organizations facilitate coordinated actions. Once an organization has processed security-related information and identified the responsible agents, it is time to orchestrate a concerted set of actions, be it preventive measures to preempt possible attacks or reparative measures to deal with the aftermath of an intrusion. Lateral organizations, being structural devices for cross-organizational unit coordination (Galbraith 1993; Joyce et al., 1997), is key to ensuring integrated and prompt actions by all those responsible units and agents.

In summary, with a "general-manager" perspective at the proper level, lateral organizations enable an organization to better discern what is going on, to decide who should do what, and to know how to do it best. In addition, each of the above three areas that lateral organizations facilitate should span across the security pillars/truss. For example, the common pitfall of treating security as a pure technical issue reflects very limited coordination along the single dimension of technology. Real coordinated actions should include the pillars. The relationship between lateral organizations and security is illustrated in Figure 1.

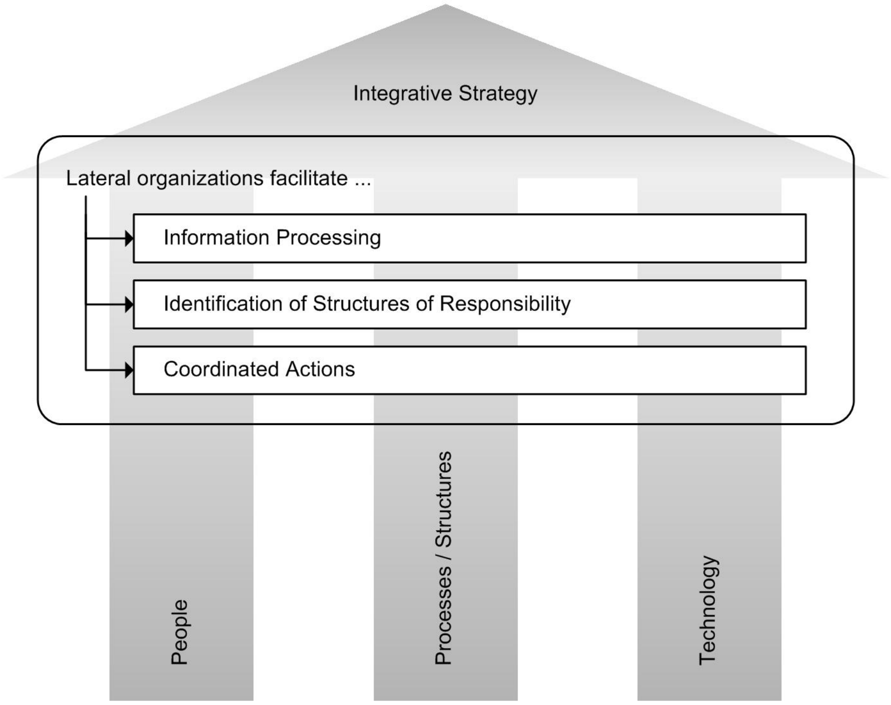

Figure 1. Lateral Organizations and IS Security

IT GOVERNANCE

The recent literature in IT governance provides insight into lateral organization specifically in the context of IT. Lateral organizations are in fact the building blocks of IT governance patterns (e.g., Weill and Ross, 2004). IT governance focuses on how decision rights can be distributed differently to facilitate centralized, decentralized, or hybrid modes of decision making.

There are some variations in the definition of IT governance (Van Grembergen, De Haes, and Guldentops, 2004). Peterson (2004) defines it as "the system by which the organization's IT portfolio is directed and controlled. IT governance describes (a) the distribution of IT decision-making rights and responsibilities among different stakeholders in the organization, and (b) the rules and procedures for making and monitoring decisions on strategic IT concerns (p. 37)."

Weill and Ross (2004) create an IT governance taxonomy that borrows six political archetypes to reflect the different distribution patterns of decision rights (cf. Weill 2004, Figure 3):

Archetype	Decision Right Distribution	Note
Business monarchy	Senior business executives make IT decisions for the entire enterprise.	The corporate IT head, the CIO, is an equal partner with other executives.
IT monarchy	IT professionals make the IT decisions.	It can be implemented in many different flavors, involving IT professionals at corporate IT or business unit IT to variable degrees.
Feudal	Business unit management makes IT decisions.	
Federal	Involving both the corporate center and business units.	It can take on one of these two broad shapes: (a) between the corporate and business unit executives but IT is not involved; or (b) either corporate IT or business IT or both can become involved in the decision.
IT duopoly	Decisions are made by the duo of IT executives and one other group, which can be either the corporate business executives or business unit leaders (Weill and Ross 2004).	This archetype also incarnate in one of these two forms: (a) "Bicycle wheel" with the corporate IT is 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 IT executive having overlapping memberships in an executive committee and an IT committee.
Anarchy	No IT governance.	

Table 3. IT Governance Archetypes

Weill and Ross (2004) suggest that there are five major IT decisions: IT principles, IT architecture, IT infrastructure strategies, business application needs, and IT investment and prioritization. For each decision type, the organization adopts an archetype as the means to obtain inputs for decisions. Empirical data show little variation in the archetypes governing input rights.

Organizations, however, differ significantly in their selected archetypes for decision rights. For instance, duopoly is used by the largest portion (36%) of organizations for IT principles decisions while for IT infrastructure decisions, IT monarchy (59%) is the most popular.

IT GOVERNANCE AND IS SECURITY

IT governance affects the quality of all five types of IT decisions (Weill 2004; Weill and Ross 2004). As a subset of IT decisions, security decisions also are subject to the reign of the instituted archetypes.

IT principles decisions are "high-level statements about how IT is used in the business" (Weill and Ross 2004, p. 27). IS security strategy sets the vision for IS security and thus is an IT principle decision. The other three practices fall within the realm of IT infrastructure, which comprises of an integrated set of ten service clusters (Weill and Ross 2004). Each key practice maps to one of the ten clusters. Top-level security policy belongs in the "IT architecture and standards" cluster. Employee security awareness has its place in "IT education," while security defense mechanisms, "infrastructure applications."

Thus, we expect that using the most appropriate IT governance archetype and its stipulated distribution of decision rights will enhance an organization's security. For example, in the feudal archetype, the business unit management has the right to make decisions. Usually lacking technical expertise, they may not be in the best position for decisions on defense mechanisms, such as where to place a firewall. A feudal archetype may not suit procedural/structural decisions, either. For instance, escalation procedures stipulate a gradient of thresholds (in terms of severity, time lapse, loss amount, etc.), each of which triggers reactions at a different organizational level (Mandia, Prosise, and Pepe, 2003). The feudal archetype is a misfit because escalation procedures involve parties in the hierarchy beyond the reach of business unit management. Some top executives, probably the CIO, must be informed for the most severe security breaches.

Generally, when the most appropriate party is authorized to make decisions, better decisions are made. The enhanced decision quality leads to higher information processing capacity, clear understanding of responsibility structures, better coordinated actions, and hence, more successful IS security. The reverse is also true.

Further, we argue that an archetype enhances IS security if it fits the decision requirements of a key practice. Duncan (1973) argues that when a decision unit's decision making structure matches the requirements of the environment, organizational effectiveness is enhanced. Next, we examine the match between the decision profile and the key aspects of security.

MATCHING DECISION PROFILES AND GOVERNANCE ARCHETYPES

A useful tool for determining how to distribute decisions in lateral organizations is the responsibility chart (Galbraith, 1973; McCann and Gilmore, 1983), a.k.a. decision rights matrix (DRM) (Korhonen and Pirttilä, 2003). The DRM technique tabulates agents in columns and decisions in rows. For each intersection cell of agent and decision, participants cast ballots on the agent's specific responsibility for that decision. At the end of the process, participants discuss their votes and arrive at a consensual distribution of decision responsibilities.

Variations exist in how researchers categorize decision-making responsibilities (Galbraith, 1973; Hinings, Hickson, Pennings, and Schneck, 1974; McCann and Gilmore, 1983; Korhonen and Pirttilä, 2003). We synthesize their taxonomies into six decision-making actions: *suggest changes* and initiate discussion about a decision, *supply information* to help decision makers evaluate alternatives, *serve as consultant*, *decide* from among alternatives, *implement* the decided course of action, and *be informed* of decision.

The DRM is a cross-section of decision structure. Duncan (1973) suggests that several types of structures may be instituted by the same decision unit for making different types of decisions. Thus, each key security practice may need a different decision profile. In Table 4 (next page), we develop an optimal profile for each practice based on a set of criteria that most likely pertain to security. It is not meant to be the "only," "best," or exhaustive set of criteria but, rather, is employed here for illustration. The criteria we use are:

(a) Fast response: Time is of the essence for most security issues. Organizations have to respond fast both in terms of understanding the problem and formulating the solution (Purser, 2004).

(b) Technical expertise: A broad spectrum of technical knowledge is a must for implementing security (Purser, 2004), as reflected by a shortage for security professionals (Clark, 2003).

(c) Synthesis of business and technical knowledge: Today's closer tie between business processes and IT requires that both business and technical skills go into security decisions (Wylder 2004).

		IS Security Strategy	**Top-Level Security Policy**	**Security Awareness**	**Security Defense Mechanisms**
I. Determination Criteria	**Fast Response**	**Low** Strategy is long-term and high level and not concerned with crises at hand.	**Low** Policy is long-term and relatively stable and not concerned with crises at hand.	**Low** Awareness programs are on-going projects and usually not directly prompted by security breaches.	**High** Time is critical to remedy of security breaches and implementation of technical tools.
	Technical Expertise	**Low** No intimate knowledge of technical details is needed for formulating strategy.	**Low** No intimate knowledge of technical details is needed for formulating policies.	**Moderate** Some technical knowledge is needed for educating employees but it does not have to be in-depth.	**High** Intimate knowledge is needed for implementing and using security tools.
	Synthesis of Business and Technical knowledge	**Moderate** Business considerations weigh more than technical ones, which are generally considered at high level.	**Moderate** Security considerations tend to weight heavier. However, business contexts should not be ignored totally.	**High** To customize awareness programs calls for knowledge of both business and technical sides.	**Low** Implementing and using security tools is generally a technical undertaking.
II. Decision Profile S = Suggest change IN = Supply information C = Consult D = Decide IM = Implement I = Be Informed		Corp Exec. (D) Corp IT (C, IN, IM) Unit Exec. (C) Unit IT (C, IN, IM)	Corp Exec. (D) Corp IT (C, IN, IM) Unit Exec. (C) Unit IT (C, IN, IM)	Corp Exec. (I) Corp IT (D) Unit Exec. (D) Unit IT (IM)	Corp Exec. (I) Corp IT (I or D, IM) Unit Exec. (I) Unit IT (D, IM)
III. Best Matching Governance Archetype		Business Monarchy	Business Monarchy	IT Duopoly	IT Monarchy

Table 4. Decision Profiles for Key IS Security Practices

These criteria are listed in Section I of the table. We rank the importance of each with respect to each of the four key security practices, which are presented as columns in the table. Based on the ranking and each agent's organizational role, authority, and capabilities, we then determine the DRM for the agents with regard to that security practice. Since governance archetypes are of concern here, the agents are corporate executives, corporate IT, business unit executives, and business unit IT. Each cell in Section II (the shaded row) represents a DRM for one of the four key security practices. Finally, we match that decision profile to a governance archetype. If this matching archetype is currently implemented for that specific security practice, then no discrepancy exists and the practice has a good chance for success. Otherwise, the current governance archetype may hinder the best result of that practice.

For instance, we propose that a business monarchy is the fitting archetype for IS security strategy. As a high-level, long-term decision, formulation of this strategy should be made by top-level executives who consider overall organizational strategies and the synergy of all organizational units. Thus, the focus is on the entire organization, rather than the business unit. The strategy must reflect environmental influences to a great extent. While some synthesis of business with technical knowledge is required, the CIO generally can provide it. The technical expertise required is relatively low and can be supplied by the

CIO and unit IT managers, who also ultimately implement the strategy. Hence, there is a proper alignment of the security practice and the decision right distribution instituted by the monarchy archetype. Misalignment would result if IT monarchy were used instead, because it would put the decision rights solely in the hands of corporate or business unit IT, which lacks the experience in and vision for organization-wide strategy issues.

In contrast, security defense mechanisms decisions often are made in response to imminent threats. The response must be fast and a high level of technical expertise is required to contain the threats. Little synthesis with business considerations is required since the decision is predominately a technical one. Depending on the situation corporate or business unit IT may make and implement the decisions "at the scene" and inform C-level and business unit executives when appropriate. In this situation, an IT monarchy archetype is suggested because of the heavy technical orientation of the decision.

Similarly, top-level security policy and security awareness decisions must take into account different determination criteria and decision profiles, as indicated in Table 4. Therefore, we propose that

> *For a given key security practice, different IT governance archetypes differentially influence its effectiveness. Best results tend to happen when the IT governance archetype matches the decision profile that is optimal for that practice.*

DISCUSSION

Often security is an issue for top-level managers only when they realize that there has been a breach within their organization. When such a breach becomes evident, fingers are usually pointed at the CIO and a technical solution is sought. Seldom is security recognized as a managerial issue that requires the involvement of many levels of management. Our IS Security Architecture framework is built upon the pillars typically noted in IS security literature: people, structures and processes, and technology. For each pillar we highlight important security practices. However, it also stresses the importance of the integrative truss, IS security strategy. The decision profiles in Table 4 are especially salient because they demonstrate that security decisions must be mindfully distributed among the organization's managers. The manner in which the decision rights are distributed varies depending upon the nature of the architectural components and decision criteria involved. Nonetheless, our decision profiles offer a starting point for sharing the important responsibility.

This paper marks our first step in exploring the important relationship between decision right distribution and IS security. Next in our research agenda, we will select variables to measure key security practices, effectiveness of IS security, and decision right distribution. Research model and testable hypotheses will then be designed in line with the relationships proposed here. We will then collect empirical data and use them to test the hypotheses and validate the research model.

CONCLUSION

Our IS Security Architecture framework and Decision Profiles contribute to the understanding of IS security by examining the relationship between security and an important part of organizational life – decision making and distribution of decision rights. Thus, social and organizational factors should be integrated into the IS security mosaic.

We identify three pillars that bolster IS security – people, processes/structures, technology, as well as the truss – the security strategy that integrates the three. Each component in our IS Security Architecture and its related security practices calls for right decisions. Lateral organizations enhance decision making and facilitate security success. IT governance is the latest perspective in studying lateral organizations in the IT context. Using Weill and Ross' (2004) taxonomy of governance archetypes, we posit that IT governance archetypes affect IS security success. We further posit that whether a governance archetype is conducive to security success depends on the match, or lack thereof, between the archetype and the ideal decision profile that a security practice requires. Selecting a governance archetype that matches the profile is critical.

REFERENCES

1. Backhouse, J. and G. Dhillon (1996) Structures of responsibility and security of information systems, European Journal of Information Systems, 5, 2-9.
2. Boyce, J. G. and D. W. Jennings (2002) Information Assurance: Managing Organizational IT Security Risks, Butterworth-Heinemann, Woburn, MA.
3. Brainbench and Information Technology Association of America (ITAA) (2003). Brainbench/ITAA Global Cyber Security Survey 2003.
4. Business Software Alliance (BSA) and Information Systems Security Association (ISSA) (2003). BSA-ISSA Information Security Study Online Survey of ISSA Members.

5. Clark, D. L. (2003) Enterprise Security, Addison-Wesley, Boston, MA.
6. Computer Security Institute (CSI) and Federal Bureau of Investigation (FBI) (2002). Computer Crime and Security Survey 2002.
7. Computer Security Institute (CSI) and Federal Bureau of Investigation (FBI) (2004). Computer Crime and Security Survey 2004.
8. Day, K. (2003) Inside the Security Mind: Making the Tough Decisions, Prentice Hall, Upper Saddle River, NJ.
9. Dhillon, G. (2001) Challenges in managing information security in the new millennium, in G. Dhillon (Ed.) Information Security Management: Global Challenges in the New Millennium, Idea Group Publishing, Hershey, PA, 1-8.
10. Dhillon, G. (2001) Principles for managing information security in the new millennium, in G. Dhillon (Ed.) Information Security Management: Global Challenges in the New Millennium, Idea Group Publishing, Hershey, PA, 173-177.
11. Dhillon, G. and J. Backhouse (2000) Information system security management in the new millennium, Communications of the ACM, 43, 7, 125-128.
12. Dhillon, G. and J. Backhouse (2001) Current directions in IS security research: Towards socio-organizational perspectives, Information Systems Journal, 11, 127-153.
13. Duncan, R. B. (1973) Multiple decision-making structures in adapting to environmental uncertainty: The impact on organizational effectiveness, Human Relations, 26, 3, 273-291.
14. Ernst & Young LLP (2004). Global Information Security Survey 2004. Chicago, IL.
15. Galbraith, J. R. (1973) Designing Complexing Organizations, Addison-Wesley, Reading, MA.
16. Galbraith, J. R. (1993) Competing with Flexible Lateral Organizations, Addison-Wesley, Reading, MA.
17. Hinings, C. R., D. J. Hickson, J. M. Pennings and R. E. Schneck (1974) Structural conditions of intraorganizational power, Administrative Science Quarterly, 19, 22-44.
18. Joyce, W. F., V. E. McGee and J. W. Slocum (1997) Designing lateral organizations: An analysis of the benefits, costs, and enablers of nonhierarchical organizational forms, Decision Sciences, 28, 1, 1-25.
19. Kankanhalli, A., H.-H. Teo, B. C. Y. Tan and K.-K. Wei (2003) An integrative study of information systems security effectiveness, International Journal of Information Management, 23, 139-154.
20. Korhonen, K. and T. Pirttilä (2003) Cross-functional decision-making in improving inventory management decision procedures, International Journal of Production Economics, 81-82, 195-203.
21. Kotulic, A. G. and J. G. Clark (2003) Why there aren't more information security research studies, Information & Management, 41, 597-607.
22. Luftman, J. and E. R. McLean (2004) Key issues for IT executives, MIS Quarterly Executive, 3, 2, 89-104.
23. Mandia, K., C. Prosise and M. Pepe (2003) Incident Response and Computer Forensics, McGraw-Hill/Osborne, Emeryville, CA.
24. McCann, J. E. and T. N. Gilmore (1983) Diagnosing organizational decision making through responsibility charting, Sloan Management Review, 24, 2.
25. Mulder, M. (1960) Communication structure, Decision structure and group performance, Sociometry, 23, 1, 1-14.
26. Peltier, T. R. (2002) Information Security: Policies, Procedures, and Standards, Auerbach Publications, Boca Raton, FL.
27. Peterson, R. R. (2004) Integration strategies and tactics for information technology governance, in W. V. Grembergen (Ed.) Strategies for Information Technology Governance, Idea Group Publishing, Hershey, PA, 37-80.
28. Purser, S. (2004) A Practical Guide to Managing Information Security, Artech House, Boston, MA.
29. Simon, H. A. (1960) The New Science of Management Decision, Harper & Brothers Publishers, New York, NY.
30. Van Grembergen, W., S. De Haes and E. Guldentops (2004) Structure, process and relational mechanism for IT governance, in W. V. Grembergen (Ed.) Strategies for Information Technology Governance, Idea Group Publishing, Hershey, PA, 1-36.
31. Weill, P. (2004) Don't jut lead, govern: How top-performaing firms govern IT, MIS Quarterly Executive, 3, 1, 1-17.
32. Weill, P. and J. W. Ross (2004) IT Governance: How Top Performers Manage IT Decision Rights for Superior Results, Harvard Business School Press, Boston, MA.
33. Whitman, M. E. (2003) Enemy at the gate: Threats to information security, Communications of the ACM, 46, 8, 91-95.
34. Whitman, M. E. (2004) In defense of the realm: Understanding the threats to information security, International Journal of Information Management, 24, 43-57.
35. Wylder, J. (2004) Strategic Information Security, Auerbach Publications, Boca Raton, FL.