

Information Security in Value Chains: A Governance Perspective

Completed Research Paper

Ravi Patnayakuni

University of Alabama in Huntsville
ravi.patnayakuni@uah.edu

Nainika Patnayakuni

Calhoun Community College
npatnayakuni@calhoun.edu

Abstract

As supply chains become more complex and global, organizations increasingly rely on advanced information technology systems to coordinate and support value chain activities. These interorganizational systems while integral to supply chain management also introduce an additional point of vulnerability. Although a matter of increasing concern, who and how the responsibility for securing these systems is governed is not well understood. We propose a conceptual framework for how these security decisions can be made in different types of value chains by combining value chain governance archetypes with the information security governance decisions that need to be made for different contexts.

Keywords

security, governance, supply chain, value chain

Introduction

With complex supply chains that cross national and organizational boundaries, each organization has less and less control of what goes out and what enters into its own supply chain. Global supply chains are now a part of the war on terror as the focus has shifted from the things taken out of the supply chains to the things put in the supply chain that pose a threat to security. Supply chain security requires the “application of policies, procedures, and technology to protect supply chain assets from theft, damage, or terrorism, and to prevent the unauthorized introduction of contraband, people, or weapons of mass destruction into the supply chain” (Closs and McGarrell 2004, p. 8). Not surprisingly the issue of securing supply chains has generated considerable interest in both practice and research and is emerging as a multi-disciplinary area of research (Gould et al. 2010; Williams et al. 2008; Lee 2004).

Organizations increasingly rely on advanced information technologies and digital platforms to coordinate their value chain activities. Although there is increasing interest on the issue of supply chain security, apart from the cautionary anecdotes highlighting the gravity of the issue, not much is said about securing information and information technology (IT) systems in the context of value chains. The recent breach of credit and debit card data at Target attracted much attention in the media. According to reports, the initial intrusion into Target’s systems could be traced back to a third party vendor for refrigeration and HVAC systems (Newman 2014). The incident underscores our use of the term ‘value chain’ rather than supply chain, even though we refer to and draw upon supply chain literature. Use of the term value chain takes into consideration variants of interorganizational relationships beyond the supply chain context such as, outsourcing and various other external entities, which may be other businesses, individual customers or the government (Dutta and McCrohan 2002). Approaching information assurance and cybersecurity from a value chain perspective emphasizes the importance of not only protecting activities in the internal value chain, but, interactions with other organizations in its ecosystems. While partnership has been an extensively studied topic in research (Patnayakuni et al. 2006), and coordination with value chain partners has been considered a sine qua non for implementing security (Closs and McGarrell 2004), organizations are often woefully unaware of what their partners are even doing as far as security is concerned.

IT governance decisions focus on who makes IT decisions and how are these decisions made in an organization (Weill 2004). These decisions could be related to what technologies to invest in, what standards to enforce, what information to share and how to integrate applications across the value chain. Investment in technologies is considered key to implementing value chain security whether these are technologies such as, RFID (Radio Frequency Identification), or an understanding and coordination of what value chain members are doing about firewalls, anti-virus, encryption programs and information security policies. Frameworks and standards have also been developed to guide the management and governance of IT security ranging from the general Control Objective for Information and Related Technology (COBIT) to the more specific ISO 27000 series that provides guidelines for information security management within the organization and ISO 27036 that deals with information security with value chain partners. Standards such as, ISO 27036 enable organizations to manage not only security related to malware, compliance, communication and networks but, also security related to partner relationships and delivery management. Section 15 of this standard on partner relationships, which was new in 2013 requires that organizations have policies, and procedures in place to protect their information that is accessible to partners as well as audit delivery of services from value chain partners.

In a global value chain, integrating and coordinating these federated and distributed security decisions is not a one size fits all approach. Research on valuechain governance looks at how value chains are managed from arms-length relationships, to partnerships and centralized hierarchies. For any given organization, its relationship with different value chain partners may require different approaches to governance. Some approaches to managing security will be more appropriate with partners while other approaches will be more appropriate for turn-key and captive partners. A better understanding of the governance of value chain security decisions is required to provide a best practice model of how organizations should approach the question of managing security in their value chain. There needs to be coordination, communication and information sharing between members in the organization's value chain (Helferich and Cook 2002) regarding information security and technologies and systems that instantiate and enforce this security. Information security governance in value chains will draw from our understanding of IT governance and governance of value chain systems as well as the socio-technical issues related to information security. In this paper we develop a framework for governance of information security across organizations in the value chain.

IT Governance

Weill (2004) defines IT governance as “specifying the framework for decision rights and accountabilities to encourage desired behavior in the use of IT”. They argue that governance is not about specific decisions about IT in the organization rather about who makes what decisions, who has input and how the decision makers are held accountable. Effective governance, according to them, is not only about ensuring compliance with the organization's policies, procedures, principles and vision but, to ensure consistency with its strategy while fostering creativity and resourcefulness of all its employees in using IT. The IT Governance Institute publishes COBIT, a framework for governance and management of enterprise IT. The framework provides detailed and comprehensive guidelines that are operationally focused around implementation and control. Other view governance as ways in which individuals and organizations solve the problem of coordination that can refer to routine operational coordination, but, is generally viewed in a strategic context (Markus and Bui 2012).

The role of IT strategy, IT architecture, IT infrastructure, business application needs and investment decisions are considered to be the five key domains of IT governance (Weill 2004). Who, where and how these decisions are made in an organization is one of the key issues in IT governance, whether these decisions are centralized or decentralized. Decision archetypes for making these decisions can range from business monarchy, IT monarchy, and federated systems all the way to disjointed feudal decision making and anarchy (Weill 2004). The research showed that profitable organizations tend to rely on centralized structures, fast growing organizations relied on decentralized structures and an asset management focus was associated with federated hybrid structures for IT governance. For organizations with a multinational footprint, Sia et al. (2010) develop a model for structuring global IT resources that meet their needs for scale and responsiveness that include shared IT services, centers of excellence and IT value managers. Sharing IT services that are resource intensive enable organizations to meet the needs of scale through outsourcing, standardization and consolidation. Centers of excellence focus on knowledge and expertise

pooling and best practice sharing across the global organization. IT Value managers bridge the gap between the local and the global by maintaining local relationships to champion local IT issues while enabling implementation of global systems.

Research on IT governance in the interorganizational context is relatively sparse. Markus and Bui (2012) review theories based on governance of social services networks, financial exchanges and business alliances to examine the governance of interorganization coordination hubs. Chatterjee and Ravichandran (2013) examine governance of interorganizational systems in terms of financial and transactional governance. Other argue that in global organizations and value chains, IT governance decisions are likely to be federated (Peterson 2004). In federated decision structures the infrastructure decisions are centralized while the application or technology use decisions may be decentralized (Brown and Magill 1998). Federated governance models present challenges in coordination and conflict resolution as the locus of control of decision making is dispersed. While standardization and service level agreements (SLA) can provide some level of vertical integration in federated environments, horizontal integration is needed to manage these distributed, dispersed decisions (Brown 1999; Peterson et al. 2000). Horizontal integration capabilities refer to the coordination of IT decisions made across business unit and organizational boundaries. Eventually effective governance is realized through deliberately and strategically designed governance mechanisms such as, committees, budgeting and approval processes, structure of the IT organization, charge back mechanisms etc. (Weill and Woodham 2003). While Weill and Ross (2005) propose decision making structures, alignment processes and formal communications as a framework for these governance mechanisms, others have proposed structure, process and communication (Ehsani and Lorenzo 2008) and similarly structure, process and people (Ko and Fink 2010). Drawing on the broad themes we propose structure, process and relational (Peterson 2004) IT governance as an appropriate framework that can be applied to examining information security in value chains. Organizations can use structural components such as, teams and liaison roles; process components such as, standardization and codification of the decision making process; and relational components such as, common learning and consensus building to manage federated security decision across the value chain.

IT Security Governance

The need for governance of information security in organizations has been recognized by both research and practice (Information Technology Governance Institute 2001; Straub et al. 2008). Information security governance has been conceptualized as either a subset of IT governance or corporate governance in organizations (McFadzean et al. 2007) or extending the already accepted definitions of IT governance (Allen 2005). Technical solutions are required but, not sufficient in meeting the challenges such as, loss of intellectual property, malicious attacks, information breaches and compromise of reputation. There is a need to move away from only technical and engineering centric approaches to security to enterprise based, “risk management, organizational continuity and resilience perspective” (Allen 2005, pg.29). Even though most organizations understand the importance of information security, they continue to view it as a technical issue solely under the purview of the IT function. Information security is a management issue that requires an end to end view of the business processes (Dutta and McCrohan 2002). In value chains the governance of information systems is not under the control of a single organization because of its inherent complexity but, a responsibility shared across organizations (Holgate et al. 2012). The inherent architecture of the Internet, its use as a platform for commerce and the often extensive value chain partnering network make it difficult to identify and define the boundary of an organization’s information systems.

There are a variety of information security governance frameworks available but, there is not one that is predominant (Holgate et al. 2012). Already mentioned here, frameworks like COBIT and ISO provide normative standards, models and practices for governing information security. In the context of value networks the responsibility for governance of security is rarely resident with single organization. Not surprisingly in value chain relationships, the web of trust plays a significant part in information security and management of relationships and often seems to be the primary means of security governance (Williams et al. 2008). While trust could be an important precondition, ensuring security will require the coordination, communication and collaboration based on multilateral relationships across organizational boundaries. Governance of information security will necessitate networked type governance mechanisms

with shared responsibility and accountability. In addition, third party providers, standard setting institutions and government agencies would likely play a role in developing interorganizational structures, processes and relational imperatives for governance in the value chain network.

Value Chain Governance

Governance in an interorganizational context has been an issue examined from several different disciplinary perspectives. Gulati and Singh (1998) identify three forms of governance as contracts, minority equity investments and joint ventures. Earlier Pisano and Teece (1989) studied R&D consortia, which could be considered as fourth form of governance (Markus and Bui 2012). In their analysis, Markus and Bui (2012) also identify related work by Provan and Kenis (2008) on governance of social services networks in public administration. Provan and Kenis identify three forms of governance, which could be considered relevant to value chain networks as participant-governed networks, lead organization governance and governance by network administrative organization, which is an administrative entity solely for the purpose of coordinating others without participating in actually delivering services. The last form of governance would be very similar to the call for third party coordination in supply chains by Bitran et al. (2007). Chatterjee and Ravichandran (2013) draw upon resource dependence theory to examine financial and transactional governance of interorganizational systems.

In this paper we use the theoretical typology developed by Gereffi et al. (2005) to propose our framework for information security governance. They draw upon transaction cost economics, production networks, and technology capability and firm-level learning to identify three critical variables – complexity of transactions, ability to codify transactions and capabilities of the supply-base - to explain patterns of governance in global value chains. Gereffi et al. argue that based on the degree of explicit coordination and power asymmetry, supply chain governance can be characterized on a spectrum where markets would be at one end of the spectrum and hierarchies at the other end. Based on their theory they propose five governance archetypes for global value chains as markets, modular, relational, captive and hierarchy. Market relationships have low switching costs while hierarchies would be characterized by managerial control and vertical integration. Where there is limited explicit coordination in market based transactions, hierarchies would be associated with the need to extensively share and control tacit knowledge. The three intermediate archetypes of modular, relational and captive value chains represent different configurations of the three critical variables.

Organizations maintain long term partnerships with other value chain members when they engage in complex transactions with capable suppliers but, find that intangible and tacit knowledge issues make it difficult to codify the handoffs from the value chain relationship in relational value chains. Modular value chains consist of turn-key suppliers who make products, which require relation specific investments but, do not require any transaction specific investments for the value chain. In modular value chains tacit knowledge is hidden in the specifications of the module. When the ability to codify transactions is high, organizations are likely to have a modular relationship with their value chain partners. But when the ability to codify is high, but, suppliers are not very capable, they are governed as captive suppliers. Captive suppliers are likely to make significant transaction specific investments in the relationship and are dependent on their customer for knowledge based activities, technology upgrades and complex design tasks. We use the factors of complexity, codification and supplier capability maturity that define the archetypes of value chain governance to define the nature of information security decisions. The degree of control, coordination and collaboration in information security decisions in value chains depends on the complexity of the security decision, the ease with which it can be codified and the maturity and capability of the supplier in information security. Table 1 provides examples of the complexity, codification and capability maturity of suppliers for information security transactions. Figure 1 then presents how the three variables will influence information security decisions across the five types of governance archetypes adapted from Gereffi et al. (2005).

Complexity of Decisions	Uncertain information security risks, high risk and or value of intellectual property or information theft
Ability to Codify Decisions	Security goals, standards and policies and compliance obligations can be clearly defined
Supplier Capability Maturity	Supplier has a validated plan to identify and protect information security assets, including vulnerability assessments. Supplier has a business continuity plan

Table 1. Characteristics of Information Security Decisions






Value Chain Governance	Information Security Decisions		
	Complexity	Codification	Supplier Capability
Market	Increases 	Increases	Increases
Modular			
Relational			
Captive		Increases	Increases
Hierarchy			

Figure 1: Information Security Decisions in Different Value Chain Governance Types

Conceptual Framework

Combining value chain governance types with information security governance decisions that need to be made, we have developed a conceptual framework of how these security decisions should be made in different types of value chains. Governance of security decisions across the value chain is likely to be dependent on both the nature of those decisions characterized by their complexity, codification and supplier maturity and the nature of value chain governance archetypes.

In most cases the governance of security decisions will flow from the governance of the value chain relationship. For example in market based relationships, organizations should be able to codify and outsource their decisions to their global suppliers without much detailed intervention and coordination. Security decisions can be standardized using the ISO 27000 series framework and the codification of those decisions using standards would enable organizations to better coordinate with their arms-length suppliers. Standardization of transactions would work as a process mechanism for horizontal information security governance in value chains. Cross functional teams and liaison roles could be used as structural mechanisms to coordinate security decisions in modular and relational value chains. Other formal mechanism that institutionalize processes for making IT security decisions such as, frameworks,

methodologies, and rules for review and service level agreements would be applicable in certain value chain contexts. Relational coordination mechanisms for value chain security would include colocation, frequent communication, high level of trust, with low power asymmetry, shared learning, knowledge and information sharing, and common goal setting routines. Table 2 provides examples of the governance mechanisms for coordinating information security decisions in the value chain.

<ul style="list-style-type: none"> • Structural integration <ul style="list-style-type: none"> ○ Institutionalized teams and inter-organizational liaison roles with suppliers to make decisions related to IT infrastructure and value chain security ○ Right to audit and compliance control by focal firm ○ Clear ownership, accountability and responsibility for the protection of valuable information assets, including security logs, audit records and forensic evidence
<ul style="list-style-type: none"> • Process integration <ul style="list-style-type: none"> ○ Standards such as, ISO 27000 series ○ Define formal processes for risk analysis, security design, identity and access management, incident management and business continuity
<ul style="list-style-type: none"> • Relational integration <ul style="list-style-type: none"> ○ Trust environment with shared responsibility for information security ○ Shared responsibility for design of policies and compliance
<p>Table 2: Information Security Governance Mechanisms in Value Chains</p>

In global value chain hierarchies with common ownership, value chain security decisions can be coordinated by both structural and relational mechanisms. The necessity for codification and standardization of every aspect of governance and security decision making is likely to be lower than in hands-off relationships and will also be limited by the inability of hierarchies to codify every aspect of the transaction due to the predominance of tacit knowledge in the relationship. Organizations that deal with intellectual property that has a very high value, work in cutting edge technologies where security risks and attack methods are uncertain and do not have suppliers with mature information security governance are likely to insource their security decisions.

In markets and modular value chains locus of control for security governance decisions is likely to be decentralized to value chain partners. Main source of coordination would be process integration - the formalization and codification of security related rules at points of handoffs between organizations. In market based exchange, since many relationships are transitory, formalization would be minimal and security need not to be managed with reliance on third parties for audit and certification. In contrast, in modular value chains, because the complexity of transactions is higher, which entail higher risk of information leakage and potential security vulnerabilities, organizations can use other process coordination mechanisms such as, formal process and standard reviews and SLAs.

In relational value chains locus of control for security decisions will be shared between value chain partners. Informal trust and shared understanding provide the basis for security governance decisions. Organizations could also rely on structural means of integration such as, cross functional teams. The use of structural mechanisms such as, cross functional teams allows for frequent communication and interaction routines that enable the development of shared understanding of value chain security. In captive value chains the controlling organization can enforce security decisions with process standardization and formalization. The conceptual framework is presented below in Table 3.

Value Chain Governance	Locus of Control	Structural Integration	Process Integration	Relational Integration
Market	Decentralized	Low	Low Standards	Low
Modular	Decentralized	Low	Medium High Standards, SLA's Process Reviews	Low
Relational	Shared	Medium Not authority but Cross-Functional Teams	Low -Medium Inability to codify value chain transactions Formal Processes	Trust Information Sharing' Common Goals
Captive	Centralized	Medium Authority and focal organization directed security initiatives	High Standards, SLA's and Frequent Process Reviews	Low
Hierarchy	Centralized	High Formal Authority	Low standardization, varying levels of rules and process reviews for decision making	Medium-High Frequent communication Common Goals Information Sharing

Table 3: Information Security Governance for Value Chains

The locus of control for information security decisions would range from centralized for hierarchies and captive organizations to decentralized for market based and modular organizations. When organizations decide to outsource their products and services to global value chains there are situations where value chain governance archetypes defined by transaction characteristics mismatch with the value chain governance requirements for information security decisions. When organizations have offshore providers in the developing world they are mostly treated as arms-length market based suppliers, the only mode of information security governance is the implementation of standards such as ISO. If an organization perceived that the complexity of security transactions result in intellectual property risk or uncertainty, modular information or captive value chain governance structures may be more appropriate so that a greater degree of control may be exercised over the partners.

There may be a mismatch between a value chain partner's transactional capabilities and its information security management capabilities. Trying to formulate long term relationships with partners through trust and information sharing may backfire if the partner has poor history and lacks capabilities in developing and implementing security policy. To compensate for the lack of partner experience in security, the focal organization may choose to either increase the level of codification and standardization of its security goals or exert greater authority and control on a relational partner's information security policy. The concepts of value chain governance, information security decisions and horizontal coordination mechanisms provide organizations with a toolset to evaluate how to govern information security decisions for the value chain.

Conclusion

Information security governance is not solely about technical issues such as, firewalls, intrusion detection systems, asset identification, risk assessment and vulnerability scanning with an inward and internal focus. Besides technical risk factors, there are various organizational risk factors such as, proprietary high value information assets, intense competition, rapid growth and the signaling effect of targeting a well know organization (NDIA 2000). Value chains make it very difficult for organizations to identify the boundaries of their information system with that of their partner and supplier organizations. Information security “requires an end to end view of business processes” (Datta and McRohan 2002, p 72).

Senior management needs to pay attention to information security by providing the IT security function and role with adequate authority to participate in and control decisions related to vendor selection, outsourcing, supplier and service provide selection. They need to propagate a culture of security and balance it with availability, innovation and customer service and even more so in the case of startups organizations such as, Snapchat, Twitter etc. that are intently focused on functionality and adoption at the expense of security. Small startup organizations are unlikely to have procedures for access control, configuration management and vulnerability assessment. Security is especially likely to be a casualty in information sharing and end to end integrated organizations because adequate data and accessibility controls may not take precedence over efficiency, and flexibility.

Information security should be a critical factor in the consideration of value chain partners, not only in its own policies but, the security and business continuity policies and procedures of its first and in some cases second tier suppliers. If a partner’s plans do not meet the needs of protecting the organizations key information assets based on a threat and vulnerability assessment the organization has the option of either changing their partners or implementing different information security governance practices than those based on the value chain archetype. Usually this may take the form of either upgrading the organizations control over the partner’s information security or increasing the level of standardization and codification of information security requirements. Increased standardization and codification could also enable an organization to search for alternate suppliers or decrease the level of structural authority and control over their value chain partners.

When the coordination costs of managing a partner’s information security policies tend to be high, especially in terms of managing structural overlays, continuous process monitoring, and standardization is not feasible because of the complexity of information security decisions, organizations can choose capable and mature suppliers and develop relational trust based organizational routines for information security. When complexity and threats are not a constraining factor, arms-length market based relationships with minimally codified information security requirements may be appropriate for information security governance. When transaction complexity and ability to codify are both available to organizations the choice of a governance relationship would depend on supplier capability.

The framework for informations security governance presented in this paper draws upon literature in value chain governance, IT governance and information security governance to provide guidelines for evaluating and thinking about information security governance in value chains. Organizations may face situations where the governance mechanisms based on value chain archetypes may not match the governance requirements based on information security needs. It is possible that relational suppliers may not have maturity and capability in information security policy and implementation. Organizations that use modular or market based mechanisms with their value chain partners but, do not make any attempt to codify and standardize information security risks, make themselves vulnerable to blended attacks to their critical information infrastructure and assets. When there is a mismatch between the governance needs of the value chain and the governance needs for information security, organizations need to carefully consider their information security policies and procedures and ensure that value chain governance archetypes are extended meet their information security needs.

REFERENCES

- Allen, J. 2005. “Governing for Enterprise Security,” Technical Note CMU/SEI-2005-TN-023. PA: The Software Engineering Institute, CERT®, Carnegie Mellon University.

- Bitran, G. R., Gurumurthi, S., and Sam, S. L. 2007. "The Need for Third-party Coordination in Supply Chain Governance," *MIT Sloan Management Review* (48:3), pp. 30–37.
- Brown, C. V., and Magill, S. L. 1998. "Reconceptualizing the Context-design Issue for the Information Systems Function," *Organization Science* (9:2), pp. 176–194.
- Closs, D. J., and McGarrell, E. F. 2004. "Enhancing Security throughout the Supply Chain", *IBM Center for the Business of Government*, Special Report Series.
- Dutta, A., and McCrohan, K. 2002. "Management's Role in Information Security in a Cyber Economy.," *California Management Review* (45:1), pp. 67-87.
- Ehsani, E., and Lorenzo, O. 2008. "Making better IT decisions," *Supply Chain Management Review* (12:5), pp 40-46.
- Gereffi, G., Humphrey, J., and Sturgeon, T. 2005. "The Governance of Global Value Chains," *Review of International Political Economy* (12:1), pp. 78–104.
- Gould, J. E., Macharis, C., and Haasis, H. 2010. "Emergence of Security in Supply Chain Management Literature," *Journal of Transportation Security* (3:4), pp. 287–302.
- Gulati, R., and Singh, H. 1998. "The Architecture of Cooperation: Managing Coordination Costs and Appropriation Concerns in Strategic Alliances," *Administrative Science Quarterly* (43:4), pp. 781–814.
- Helferich, O. K., and Cook, R. L. 2002. *Securing the Supply Chain*, Oak Brook, IL: Council of logistics management.
- Holgate, J., Williams, S. P., and Hardy, C. A. 2012. "Information Security Governance: Investigating Diversity in Critical Infrastructure Organizations," in *Proceedings of the 25th Bled Conference*, June 2012, Bled, Slovenia.
- Information Technology Governance Institute. 2001. "Information Security Governance: Guidance for Boards of Directors and Executive Management.," Rolling Meadows, IL: Information Systems Audit and Control Foundation (ISACF).
- Ko, D., and Fink, D. 2010. "Information Technology Governance: An Evaluation of the Theory-practice Gap," *Corporate Governance* (10:5), pp. 662–674.
- Lee, H. L. 2003. "Supply Chain Security-Are You Ready," Stanford Global Supply Chain Management Forum, SGSCMF-W1-2004, Stanford, CA: Stanford University.
- Markus, M. L., and Bui, Q. "Neo." 2012. "Going Concerns: The Governance of Interorganizational Coordination Hubs," *Journal of Management Information Systems* (28:4), pp. 163–198.
- McFadzean, E., Ezingard, J.-N., and Birchall, D. 2007. "Perception of Risk and the Strategic Impact of Existing IT on Information Security Strategy at Board Level," *Online Information Review* (31:5), pp. 622–660.
- NDIA. 2000. "Computer Network Defense: An Industry Perspective, an NDIA study in support of US Space Command (Unclassified)," National Defense Industry Association.
- Newman, L. H. 2014, February 6. "Target's Heating and Refrigeration Company Gave Hackers the Key to Customer Data," *Slate*, Online Magazine (<http://www.slate.com/blogs/future-tense/> accessed February 24, 2014).
- Patnayakuni, R., Rai, A., and Seth, N. 2006. "Relational Antecedents of Information Flow Integration for Supply Chain Coordination," *Journal of Management Information Systems* (23:1), pp. 13–49.
- Peterson, R. 2004. "Crafting Information Technology Governance," *Information Systems Management* (21:4), pp. 7–22.
- Pisano, G., and Teece, D. 1989. "Collaborative Arrangements and Global Technology Strategy: Some Evidence from the Telecommunications Equipment Industry," in *Research on Technological Innovation, Management and Policy*, Vol. 4, R. S. Rosenbloom and R. A. Burelman (eds.), Greenwich, CT: JAI Press, pp. 227–256.
- Provan, K. G., and Kenis, P. 2008. "Modes of Network Governance: Structure, Management, and Effectiveness," *Journal of Public Administration Research and Theory* (18:2), pp. 229–252.
- Sia, S. K., Soh, C., and Weill, P. 2010. "Global IT management: Structuring for Scale, Responsiveness, and Innovation," *Communications of the ACM* (53:3), pp. 59–64.
- Straub, D. W., Goodman, S., and Baskerville, R. L. 2008. "Framing the Information Security Process in Modern Society," In *Information Security: Policy, Processes and Practices*, D. Straub, S. Goodman and R Baskerville (eds.), Armonk, NY: M.E. Sharpe, pp. 5–12.
- Weill, P. 2004. "Don't Just Lead, Govern: How Top-Performing Firms Govern IT," *MIS Quarterly Executive* (3:1), pp. 1–17.

- Weill, P., and Ross, J. 2005. "A Matrixed Approach to Designing IT Governance," *MIT Sloan Management Review* (46:2), p. 26–34.
- Williams, Z., Lueg, J. E., and LeMay, S. A. 2008. "Supply Chain Security: an Overview and Research Agenda," *International Journal of Logistics Management, The* (19:2), pp. 254–281.