Strategic Information Systems Security: Definition and Theoretical Model

Completed Research Paper

Andy Luse
Oklahoma State University
andyrluse@iastate.edu

Anthony Townsend
Iowa State University
amt@iastate.edu

Brian Mennecke
Iowa State University
mennecke@iastate.edu

Samuel Demarie
Iowa State University
demarie@iastate.edu

ABSTRACT

Information systems security has become a critical topic both academically and in industry due to its importance in today’s organizational environment. But while its criticality is undeniable, information systems security continues to be viewed reactively, as a “necessary evil,” or, worse, as a black hole with little or no ROI. Researchers and practitioners alike have generally been reticent to acknowledge the strategic potential of information systems security. This paper provides a first step towards helping managers justify their investments in information systems security by identifying its strategic potential. In doing so, we address three basic questions; why is information systems security important, what is strategic information systems security, and how does the strategic potential of information system security affect firm performance. Dynamic capabilities theory is utilized to propose a theoretical framework for strategic information systems security. We propose that information systems security provides the infrastructure necessary for agility, which in turn impacts firm performance. Specifically, information systems security enables sensing and responding to customer, partner/supplier, and internal organizational opportunities to positively impact firm performance. We also propose that the trust generated by solid security and security policy can enhance relationships with both customers and partners/suppliers.

Keywords

strategic information systems security, information systems evolution, agility, strategic information systems, dynamic capabilities theory

INTRODUCTION

Information systems security has been an area of considerable attention for information systems (IS) managers for a number of years. Information systems security was first presented as a relevant topic and as a potential focus for IS research in 1987 (Brancheau and Wetherbe, 1987). Since that time, security concerns have continued to grow in significance as corporations have become even more interconnected and utilize networks for a greater number of organizational functions. Furthermore, part of the implication of operating a business in the “digital age” is that information about most corporate assets are digitally archived. While digitalization offers powerful advantages and numerous benefits, it also creates risks because of the relative ease of duplication, corruption, or theft of digitally represented assets and resources. As a consequence, IS security represents a foundational capability in most organizations because of the dependence on digital assets and the simultaneous need to position these assets on networks that are exposed to external agents (e.g., business partners, customers, etc.). Recent surveys such as the Computer Security Institute Computer Crime and Security Survey show a continued desire by corporate security administrators for greater investments and resources for network security administration (Richardson, 2009). Research has also suggested that organizations have been reporting a greater number of information systems security breaches as well as security incidents from within the organization (Dhillon and Torkzadeh, 2006), which further emphasizes the critical nature of corporate network security. With new threats of cyber-terrorism and corporate espionage increasing, the importance of information systems security is greater than ever.

While the importance of information systems security in the corporate environment is evident, the strategic potential of information systems security remains unexplored. Most corporate information systems specialists and researchers alike see information systems security as reactive in nature and a necessary cost of doing business. Information systems security is
generally evaluated for its deterrent and preventative properties (Kankanhalli, Teo, Tan, and Wei, 2003) and not for the strategic advantage it can potentially offer. Some studies have begun to explore the value added by information system security (Dhillon and Torkzadeh, 2006), but no research to date has looked at the strategic potential that information systems security can hold and its capability for contributing to competitive advantage and firm performance. An important question is whether a failure to recognize the strategic potential of information systems security might lead to a loss of revenue, a failure to develop competitive competencies, and a diminished potential to achieve a competitive advantage.

This research provides an important first step towards understanding information systems security from a strategic perspective and the mechanisms by which information systems security influences firm performance. The goal is to provide firms with a theoretical lens through which they can view information systems security as a strategic asset and utilize information systems security to positively impact firm performance. To do this, three questions must be answered. First, **why** is fundamental information systems security itself important? As with any initial research into an area, it is critical to first establish the context for research in the topic and a link must be established between information systems security and firm performance to warrant further investigation. Second, **what** is **strategic** information systems security? After the importance of information systems security has been established, the case must be made that information systems security is not only important, but **strategically** important. To answer this question, a historical perspective is taken and parallels are drawn with strategic information systems to both understand the historical trajectory of information systems security and to propose a future definition for **strategic information systems security**. Third, **how** does strategic information systems security influence firm performance? Assuming that the first two questions are answered affirmatively, the method by which information systems security **strategically** impacts the firm must be understood in order to demonstrate that there is an imperative for adopting a strategic information systems security perspective. We will explore the effect of information systems security and trust on corporate agility, which in turn affects firm performance. This analysis then articulates the need for firms to adopt a proactive and strategic view of security to enable superior performance through a responsive and secure information systems infrastructure.

**WHY IS INFORMATION SYSTEMS SECURITY IMPORTANT?**

Before proceeding further, it is essential to first make a case for the importance of information systems security, as only then does it make sense to proceed towards an articulation of **strategic** information systems security. This section provides research exemplars pointing towards the importance of information systems security which, when taken together, provides a basis on which the potential for information systems security can be viewed strategically.

Information systems are ubiquitous in organizations and almost all aspects of an organization’s operations utilize some sort of information systems technology. As organizations continue to increase their dependence on information systems for strategic advantage, information systems security will play an increasingly important role within organizational systems (Kankanhalli, et al., 2003). Research has shown that investments in information systems security can offer strategic complements by creating positive externalities (Anderson and Moore, 2006; Kunreuther and Heal, 2003). For example, by adopting more stringent security practices, a firm influences other corporations to do the same. Furthermore, as top management teams are incorporating information systems into their business strategies, information systems security has been shown to be as important strategically as the operational systems that firms traditionally have relied on to perform day-to-day operations (Kotulic and Clark, 2004).

Historically, researchers and managers alike have regarded information systems security for its preventative and deterrent capabilities both for internal operations as well as for defending against external threats (Straub and Welke, 1998). Within the organization, preventative efforts attempt to ward off nefarious behavior through the use of controls (Forcht, 1994) and are the next line of defense if deterrent efforts fail (Straub and Welke, 1998). Information systems security requires continual development to prevent abuses which can potentially lead to competitive disadvantage, providing a strong rationale for protecting computer systems (Gupta and Hammond, 2005). Research has shown that firms experience significant losses resulting from IS security breaches when information systems security is not given a priority position in the firm’s operational plans (Cavusoglu, Mishra, and Ragunathan, 2004; Kadrosky, 2000; Richardson, 2009). Evidence further suggests that even the market value of a firm is linked to its security performance, which reflects on the external stakeholders’ views about the degree of inherent firm-specific risk associated with the firm and is representative of a firm’s potential for future financial losses (Cavusoglu, et al., 2004).

Legal troubles also provide a strong incentive for investments in security for many firms as liability lawsuits are expected to rise for those organizations that have exhibited lapses in security (Gupta and Hammond, 2005). Investments in security can prevent catastrophic losses from liability suits because of careless security practices (Bharadwaj, Bharadwaj, and Konysnski, 1999). In addition to improving the security function, other security related enhancements include better policy, legitimate
use guidelines, and audits of information systems assets (Straub, 1990). These security investments can also help to dissuade nefarious activity on the corporate network through fear of sanctions such as lawsuits and loss of employment (Forcht, 1994).

Consumer trust is another factor which is improved with greater information systems security, which is especially true for firms that engage in online transactions (e.g., firms with an e-tail presence). By increasing consumer perception of corporate security prowess, perceived corporate reputation increases, which in turn increases trust (Jarvenpaa, Tractinsky, and Vitale, 2000). Security perceptions have been shown to be one of the key drivers of online trust (Hoffman, Novak, and Peralta, 1999), (Dayal, Landesberg, and Zeisser, 1999). Further, even corporate policies toward security are found to improve consumer online trust (Schneiderman, 2000). Finally, the relationship between information systems security and the valuation of the firm in the market can be at least partially explained by the trust consumers place in the corporation (Cavusoglu, et al., 2004).

WHAT IS STRATEGIC INFORMATION SYSTEMS SECURITY?

The previous section establishes the importance of information systems security vis-à-vis firm performance, and with the importance of information systems security determined, we will further define this importance as strategic in nature and positively linked to the valuation of the firm and the strategic alignment thereof. Consequently, we now define the concept of strategic information systems security.

As noted above, most professionals and scholar view security as a necessary cost of doing business, not as a strategic asset; therefore, there is a dearth of extant research in this domain. Given this, the case must be made through analogy with other, related systems and by logical argumentation. We will present both of these arguments, respectively. First, by way of analogy, the primary related research domain is clearly the research that has examined strategic information systems (Reponen, 1993; Ward, Griffiths, and Whitmore, 2002). Information systems followed a progression of evolutionary developments before it could be defined as being strategically important. To develop a definition of strategic information systems security, we must therefore first determine that information systems security is far enough along its evolutionary path to be considered a strategic asset. Once this case is presented, we can then proceed with offering a definition of strategic information systems security. Also, by first deciphering where we are at in the developmental process, we can also better propose a trajectory for action designed to achieve this strategic role of information systems security. Specifically, this will be achieved through the development of a framework by which strategic information systems security can be shown to positively affect firm performance. Information systems generally have provided a clear example of the path toward strategic importance and we propose that information systems security will follow this same path towards a similar position of strategic importance.

Evolution of Information Systems

The view that information systems have a strategic role in organizations is now well established; yet, this has not always been true. Information systems had to transition through several phases of development within organizations before the strategic nature of these systems could be recognized and demonstrated. Specifically, information systems evolved through three broad phases or “eras” of use that are often represented in introductory information systems textbooks and specifically include 1) data processing, 2) management information systems, and 3) strategic information systems (Pant and Ruff, 1995; Ward, et al., 2002).

These eras roughly describe not only the application for which these systems were used but also the general attitudes about these systems that were held by corporate management during these respective periods in history (see Figure 1 and Table 1 for a succinct description). During the data processing era, information systems were viewed as a support mechanism for day-to-day operational tasks; these systems were seen more as a means of cost reduction due to their speed and ability to automate tasks. The management information systems era is characterized by distributed, interconnected systems and, instead of being relegated to a back room, the information system became a user-driven process designed for information distribution and collation and, further, it was used directly by management and viewed as a service supporting broad areas of the business. Finally, the strategic information systems era is characterized by networked, integrated systems that are available to and supportive of users. In this context, the information system is integrally tied to business strategy, it

---

1 It should be recognized that systems in each era had a strategic role. For example, a data processing system would be installed to reduce labor costs, speed up operations and cycle times, and reduce errors (see (Weill and Aral, 2006)) Clearly, these systems would have been viewed at the time as having a benefit to the organization and, in some cases, would have provided a competitive advantage. Nevertheless, such strategic advantages are short lived and do not describe how these systems can not only serve a strategic goal but also become integrally tied to the organizations operations, managerial, and strategic interests.
“enables” the business to digitize processes and functions, and it is business driven (Pant and Ruff, 1995; Ward, et al., 2002). While the preceding information systems functions are still a component of current technologies, information systems as a technology and, certainly, as a discipline has assumed a deserved position at the organizational strategy table.

Figure 1. Eras of Information Systems evolution

<table>
<thead>
<tr>
<th>Eras of IS Evolution in Organizations</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Data Processing</strong></td>
</tr>
<tr>
<td>Backroom operation separate from users in support of day-to-day operational tasks and cost reduction.</td>
</tr>
<tr>
<td><strong>Management Information Systems</strong></td>
</tr>
<tr>
<td>Distributed, interconnected, user-driven processes regulated by management. Viewed as a service supporting the business.</td>
</tr>
<tr>
<td><strong>Strategic Information Systems</strong></td>
</tr>
<tr>
<td>Networked, integrated systems which are available to and supportive of users, relate to business strategy, “enable” the business, and are business driven.</td>
</tr>
</tbody>
</table>

Table 1. Description of eras of information systems evolution(Pant & Ruff, 1995; Ward, et al., 2002)

Proposed Evolutionary Trajectory of Information Systems Security

The first step towards utilizing information systems security strategically is to understand the history behind it. Just as information systems has followed a three-era trajectory, information systems security can also be delineated by such a roadmap (see Figure 2 and Table 2). In its early phase, information systems security was utilized in an auditing capacity; as an example, Denning’s seminal piece on intrusion detection proposes a model for monitoring system audit records to detect information systems security breaches (Denning, 1987). Similar to information systems’ use as a data processing mechanism, information systems security was utilized primarily as a log processing system. These auditing processes were initially performed post-hoc and were used primarily as a verification mechanism for security procedures and also as a measure of system utilization. Later, these systems became more automated and real-time to better detect possible attacks as they were occurring. Next, information systems security entered the era of corporate security management. Just as
information systems was a distributed, interconnected, user-driven process regulated by management in the management information systems era, information systems security has gone through a similar parallel period of various distributed security hardware and software components utilized by management to actively protect the corporate network, thereby supporting daily business processes.

The third era of information systems security, strategic information system security, is much like strategic information systems as it allows for system integration and service availability to support exploration and exploitation of business opportunities which are aligned with the corporate business strategy. The primary difference is that while the strategic information systems era has already begun, the strategic information systems security era has yet to be widely adopted. Managers in most organizations hold to the older paradigm of security management; that is, viewed from a functional perspective where the role of these systems is primarily tools based (e.g., to protect corporate systems) and as a cost center (e.g., as a “necessary evil” for conducting business). We believe that information systems security has reached an evolutionary stage that enables strategic planning and proactive decision making capabilities and creates an imperative to move into this third era of its evolution.

![Figure 2. Proposed eras of IS security evolution.](image)

<table>
<thead>
<tr>
<th>Eras of IS Security Evolution in Organizations</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Auditing</strong></td>
</tr>
<tr>
<td>Log processing to verify security procedures and information systems usage post-hoc.</td>
</tr>
<tr>
<td><strong>Corporate Security Management</strong></td>
</tr>
<tr>
<td>Network security administrators utilize software and hardware to actively protect corporate systems and monitor data transfer.</td>
</tr>
<tr>
<td><strong>Strategic Information System Security</strong></td>
</tr>
<tr>
<td>Integrated security systems which provide secure and available services which are supportive of exploration and exploitation of business opportunities and are related to the corporate business strategy</td>
</tr>
</tbody>
</table>

*Table 2. Description of proposed eras of IS security evolution.*
While this section utilizes a historical perspective to develop a definition of the concept of strategic information systems security, the link between strategic information systems security and performance has yet to be made. Based on this articulation of the potential for a strategic information system security approach, the next section provides a theoretical framework for linking strategic information systems security with firm performance.

**HOW DOES INFORMATION SYSTEMS SECURITY STRATEGICALLY AFFECT FIRM PERFORMANCE?**

This section proposes a model of strategic information systems security and outlines propositions to connect the constructs within the model. The model itself can be viewed in Figure 3 along with links depicting developed propositions.

Dynamic capabilities theory describes a firm’s ability to “integrate, build, and reconfigure internal and external competencies to address rapidly-changing environments” (Teece, Pisano, and Shuen, 1997). Dynamic capabilities theory proposes that, to maintain a competitive advantage, firms must continually adapt their capabilities (Overby, Bharadwaj, and Sambamurthy, 2006) and within information systems, dynamic capabilities allow firms to combine different IS and business resources to potentially stimulate firm performance (Sambamurthy, Bharadwaj, and Grover, 2003). Dynamic capabilities have been described as an overarching theory that utilizes various sub-concepts, including agility; thus, while dynamic capabilities theory is relevant to all types of firm processes, agility includes only those relevant for sensing and responding to the corporate environment (Sambamurthy, et al., 2003).

Research has described agility as underlying corporate success and contributing to firm performance (Sambamurthy, et al., 2003). Due to increased rivalries from globalization, agility is considered essential for firm success (Brown and Eisenhardt, 1997; Christensen, 1997; D’Aveni, 1994; Goldman, Nagel, and Preiss, 1995) as it buttresses firm competitiveness through continual enhancement and redefinition of value creation (Sambamurthy, et al., 2003) and enhances the ability of a firm to be successful in turbulent environments (Overby, et al., 2006).

Definitionally, agility is the ability of an organization to respond quickly to changing market conditions, thereby providing the organization with a competitive advantage (Broadbent and Weill, 1997; Broadbent, Weill, and Don St, 1999; Keen, 1991; Peppard and Ward, 2004). The increased pace of business change, greater demands from customers, and hypercompetition of the market have increased the importance of firm agility (D’Aveni, 1994; Goldman, et al., 1995; Sambamurthy, 2000). Agility enhances the ability of the firm to leverage assets, knowledge, competencies, and exploit innovation opportunities (Piccoli and Ives, 2005; Sambamurthy, et al., 2003) and includes both the detection of opportunities and acting upon those opportunities in a timely manner (D’Aveni, 1994; Goldman, et al., 1995). These two areas have also been described as sensing and responding, both of which are needed to increase firm performance (Overby, et al., 2006). Action/responding includes both the exploitation of current knowledge through extension and refinement and exploration of new opportunities and knowledge (March, 1991).

Research has shown that firm investments in information technology enable enterprise agility which in turn affects firm performance (Overby, et al., 2006; Sambamurthy, et al., 2003). Information systems have been shown to have an important role in enabling sensing and responding by firms (Bradley and Nolan, 1998; Sambamurthy, et al., 2003; Weill and Broadbent, 1998). A firm must possess effective information systems to sense changes relevant to the business, including changes due to advances in information systems (Overby, et al., 2006). Furthermore, information systems enables both sensing and responding by extending the reach and richness of firm processes, communication, and knowledge (Overby, et al., 2006; Sambamurthy, et al., 2003). In effect, information systems provide the infrastructural base through which agility can influence firm performance.

Information systems security is one piece of the corporate information systems infrastructure that must also be evaluated as a performance measure of the firm (Hamilton and Chervany, 1981). Given the arguments above that information systems have the potential to support an organization’s agility, information systems security, a subcomponent of information systems, would also have the potential to contribute in supporting agility. For example, the level of efficiency of any given information systems security platform might contribute to the effectiveness of the overall IS, which in turn influences the outcomes of performance measures for the firm (Hamilton and Chervany, 1981). Stated formally...

\[ P_1: \text{Organizational agility positively affects firm performance through sensing and responding when supported by the positive effect of information systems security.} \]

Agility relies on three interconnected areas to be effective: customer agility, partner/supplier agility, and operational agility (Cronin, 2000; Tapscott, Ticoll, and Lowy, 2000; Treacy and Wiersema, 1993). Customer agility involves utilizing...
customers as a means of sensing and responding to opportunities for innovation (Sambamurthy, et al., 2003). Customers stimulate competitive response by the firm by providing innovative ideas and testing new products (Nambisan, 2002). Furthermore, customer agility describes the ability of the firm to listen to the customer for market intelligence and detect new competitive opportunities through this interaction with the customer (Kohli and Jaworski, 1990). Information systems provide a means for enhancing customer interactions and thereby increase the organization’s customer agility (Holstrom, 2001; Kambil, Friesen, and Sundaram, 1999; Nambisan, 2002).

Information systems security has been described in a reactive sense as a way of lessening the threat to damage of customer confidence (Doherty and Fulford, 2006; Menzies, 1993), thereby enabling greater interaction with customers (i.e. sensing of customer issues) and greater opportunity for customer response. Information systems security can bring about benefits for the firm by raising the confidence of the customer in the organization’s capabilities and risk profile (Anthes, 1998; Kankanahalli, et al., 2003). Value-focused thinking helps to show the net benefits and costs associated with IS security (Dhillon and Torkzadeh, 2006), which affects the confidence of customers with the corporation.

Security has been shown to increase trust of customers in the firm (Shankar, Urban, and Sultan, 2002), which then allows for greater interaction with customers, response to customer issues, and overall customer agility. Trust in a company’s security systems has been shown to affect the relationship between the customer and the focal firm (Suh and Han, 2003). This trust in the technology will eventually lead to trust in the firm itself (Siau and Shen, 2003), creating opportunities for greater communication between parties. Provision trust (i.e. trust of customers in authenticated parties and the goods and services they provide) has been shown to increase trust in perceptions of communication security customers have with firms (Josang, Ismail, and Boyd, 2007). Increasing communication security, in turn, leads to greater opportunities for sensing and responding to customers, which also contributes to agility. Security controls have been shown to lead to trust in customer websites, which, in turn, leads to customer interaction with the company (Koufaris and Hampton-Sosa, 2004).

Given this, we believe that information systems security will facilitate open and dynamic interactions with customers, which is needed for sensing and responding to customer-related issues. Nevertheless, this relationship will be moderated by the level of trust that the customer has with the focal organization. More formally stated

\[ P_2: \text{The benefits provided to customers by the organization’s information systems security will increase trust of the customer in the firm (P}_{2a}\) thereby facilitating greater customer agility of the organization and securing the relationship necessary for sensing new opportunities and responding to those opportunities (P}_{2b}. \]

Partnering agility is the firm’s ability to leverage the knowledge, assets, and competencies of partners through alliances, partnerships, and joint ventures (Venkatraman and Henderson, 1998). Through these partnerships, firms can explore opportunities for innovation and competitive action (Choudhury and Xia, 1999). Partnering agility allows the firm to utilize knowledge not currently present in their own organizational network (Dyer and Singh, 1998), which enables the firm to have better response mechanisms thereby potentially increasing performance (Zaheer and Zaheer, 1997). Information systems security facilitates the cooperation among firms for greater responsiveness to partners and coordination in engaging in mutually beneficial inter-organizational activities. By providing an effective infrastructure, information systems security facilitates interaction with partners, enabling corporations to better sense issues with these partners and respond to coordination issues effectively.

Trust has also been shown to be important for facilitating interaction between the firm and its partners and suppliers (Shankar, et al., 2002). Security can affect business based on the trustworthiness of the relationship between partners (Ratnasingham, 1998). Security implementations have been shown to enhance trust in the firm-partner relationship, which prompts the partner to interact more richly with the firm (Moorman, Deshpande, and Zaltman, 1993), thereby opening the door to greater availability of information and know-how from the partner (Ke and Wei, 2008). This openness provides for better interaction with the partner (Ratnasingham, 1998).

In considering these factors together, we believe that information systems security will enhance trust with partners and suppliers and this will facilitate greater interaction, opening the door to greater sensing and responding to the needs of partners and suppliers. Therefore, we propose:

\[ P_3: \text{The security benefits provided to partners/suppliers by the organization’s information systems security will enable the trust environment necessary for partnering agility of the organization (P}_{3a}, and encourage the} \]
development of information systems that support sensing new opportunities and responding to those opportunities ($P_{3b}$).

Operational agility describes the ability of the organization to enable exploitation of internal ideas for competitive advantage. By enabling comprehensive information systems, operational agility allows for the reduction of asymmetries between customers and partners (Sambamurthy, et al., 2003). Information systems enable operational agility by allowing the improvement and creation of new business processes (Malone, Crowston, Lee, and Pentland, 1999) and providing the infrastructure capabilities and communication channels for faster and better-informed decision-making (Amit and Zott, 2001). This infrastructure provides the basis for more effectively identifying internal issues and responding to those issues in a timely manner.

Research has shown that security is a necessary component of organizational infrastructure capabilities (Ahsan and Ngo-Ye, 2005; Broadbent and Weill, 1997; Broadbent, et al., 1999; Fink and Neumann, 2007; Peppard and Ward, 2004; Weill, Subramani, and Broadbent, 2002) which itself contributes to the overall health of the organization. These infrastructure capabilities have been described as having the ability to provide data with the necessary levels of confidentiality and security (Ahsan and Ngo-Ye, 2005), which have both been theorized and shown to significantly affect operational agility (Fink and Neumann, 2007; Sambamurthy, et al., 2003). Also, security and risk have been included in the list of the ten capabilities that are necessary for the infrastructure to support strategic agility within the organization (Broadbent and Weill, 1997; Broadbent, et al., 1999; Fink and Neumann, 2007; Weill, et al., 2002). These infrastructure capabilities enable organizational agility through sensing and responding to internal issues. Given this information, we propose

$$P_4: \quad \text{Strategically developed information systems security supporting the organization’s information systems infrastructure will allow for operational agility of the organization through sensing new opportunities and responding to those opportunities.}$$
The model represented in figure 3 diagrammatically depicts our theoretically-based propositions. Specifically, information systems security enables agility for the organization. This agility enables the organization to better sense and respond to both customer and partner/supplier issues as well as issues internal to the corporation. Trust is also shown to moderate the sensing and responding relationship between the focal firm and both customers and partners/suppliers. This information systems security enabled agility in turn leads to better firm performance. The entire model depicts the concept of strategic information systems security.

DISCUSSION

Over the past decade, the rise in threats to corporate information systems has lead corporations to place greater emphasis on information systems security, which has also lead many organizational leaders to question the value of such security procedures. Agility, a component of dynamic capabilities theory, has been shown to play a vital role in firm performance (Brown and Eisenhardt, 1997; Christensen, 1997; D'Aveni, 1994; Goldman, et al., 1995) and in the strategic role of information systems within the organization (Sambamurthy, et al., 2003). Information systems security enables this overall information systems infrastructure. The objective of this paper has been to explore the connections between information systems security and overall firm performance. Specifically, we have looked at the facilitating role of information systems security for corporate agility and the link to firm performance.

There are two important implications of this research for both academicians and practitioners. First, we have provided a proposed roadmap for information systems security towards a strategic position within the firm. This was accomplished by reviewing the history of strategic information systems and utilizing this information as a template. This roadmap is important as it provides perspective as to how information systems security has changed over time within the organization. Additionally, it provides a proposed trajectory by which information systems security will be fully realized as a strategic asset within the firm.
A second implication of this research is the development of a model of strategic information systems security. The model proposes that information systems security enables corporations to both sense and respond to opportunities in their market with greater ease, predominantly by creating the trust environment necessary for these processes to occur. By strategically orienting information systems security toward the creation of security environments that support effective partnerships with customers and other firms, the organization can better exploit opportunities in their environment which can lead to greater firm performance. Overall, the model points to information systems security as a strategic asset of the firm, an asset that creates its own value both in protection and in partner attitudes toward the firm.

The proposed model holds opportunities for future research in the area. While this research demonstrates the strategic role of information systems security as it pertains to organizational agility and trust, greater research is needed into other possible mechanisms which belong to strategic information systems security, such as other missing constructs. Also, greater research is needed into the interrelationship of the three components of agility and trust as they pertain to information systems security, with an eye toward articulating and identifying security strategies for different operating environments. Furthermore, these constructs will change over time and greater research is needed into the longitudinal nature of the model. Another area for future research involves other variables external to the model which could be affected by, or directly affect, strategic information systems security. Previous research has found that other exogenous variables can affect information systems agility (Sambamurthy, et al., 2003) and these other variables should be explored in the context of information systems security.

Finally, empirical research should be utilized to test the proposed model. These tests could involve analyzing the overall variance explained of firm performance based on strategic information systems security, both through its indirect effect through agility and trust and its effect on customer and partner good-will toward the firm. Also, the individual constructs could be tested to identify which variables within the model contribute most to overall firm performance.

CONCLUSION

The role of information systems security has changed dramatically over the past 30 years, but this story is not yet complete. We argue that information systems security has not yet been exploited to its full potential in the organization as a strategic mechanism. This research presents answers to three questions regarding information systems security: (1) why is information systems security important, (2) what is strategic information systems security, and (3) how does information systems security strategically affect firm performance. The research proposes a model which demonstrates the effect of information systems security on firm agility, trust, and overall firm performance. Specifically, information systems security provides the necessary infrastructure that enables sensing of and responding to opportunities with customers, partners/suppliers, and internal operations to better enable firm agility, which in turn contributes to more positive overall firm performance. Furthermore, information systems security enables trust which strengthens the relationships with customers and partners/suppliers. The proposed model provides both a theoretical basis for further research as well as first steps towards providing firms with a template for realizing and utilizing the strategic benefits of information systems security.

Continued research into the strategic nature of information systems security is needed. While the importance of information systems security is undeniable, greater research should explore the proposed trajectory for viewing information systems security strategically. Also, additional empirical research is needed into the proposed model and our predictions based on this theoretical framework. Our hope is to provide an impetus to greater research into strategic information systems security.

REFERENCES


