PERCEPTION AND REALITY: AN INTROSPECTIVE STUDY ON SUPPLY CHAIN INFORMATION SECURITY RISK

Gregory E. Smith, Xavier University, smithg2@xavier.edu
Kevin J. Watson, University of New Orleans, kwatson@uno.edu
Wade H. Baker, Verizon Business Solutions, wade.baker@verizonbusiness.com

ABSTRACT

The collaborative nature of supply chains has exposed firms to a variety of security risks. With information technology (IT) as the cornerstone to integration, this exposure can be passed throughout all levels of business. Unfortunately, the role one plays in the supply chain may affect an internalized view of their firm's current security position, both in terms of what is being done and what should be done to limit risk exposure. This paper provides an initial investigation of the nature and perception of information security risk in supply chains and the managerial implications and limitations of current IT security practices.

Key words: Information Security, Supply Chain, Collaboration, Risk

INTRODUCTION

As the scope and complexity of modern supply chains continue to grow, firms increasingly rely on collaborative partners for survival. This tendency has accelerated in recent years as firms increasingly leverage information technology (IT) to enhance their supply chains. By eliminating traditional layers of internal and external separation which once formed a protective barrier around a firm's assets and processes, IT-facilitated collaboration has improved customer service and satisfaction. Unfortunately, it has also increased a firm's vulnerability to an array of IT-specific risks. Thus, the intimate relationship between technology and revenue has forced decision makers to balance often opposing goals: collaboration vs. security.

Though questions relating to this balance are considered to be among the most challenging and frequently asked of the day [10], research on the topic is surprisingly sparse. Therefore, an initial investigation was conducted about the nature and perception of information security risk in supply chains. To this end, we surveyed more than 200 firms spanning various supply chain functions.

We present our findings as follows. First, we present a short literature review of collaboration and IT in integrated supply chains. This is followed by a discussion of the survey methodology. Next, we discuss the results of the survey, focusing briefly on perceptions surrounding information security risk within supply chains. We conclude with a discussion of managerial implications and limitations of current approaches.

LITERATURE REVIEW

The goal of supply chain management is to merge all value chain functions into a unified routine that stresses collaboration among partners. Collaboration, a mutual decision making process where partners share information, knowledge, risk, and profits based on a foundation of trust and commitment [14], is the central principle in creating flexible supply chains [16]. The necessity of collaboration among supply chains has increased so rapidly that research has identified collaboration as possibly the single most pressing need in supply chain management for process optimization [1].

Collaboration enables supply chain partners to exceed simple operational-level interactions and increase their competitiveness [13]. Research suggests that collaboration among supply chain partners, when facilitated by an integrated flow of information, can enhance revenue, reduce costs, and improve operational flexibility [9,11,4,15,19]. However, it is the depth and maturity of partner relationships, information sharing, and IT integration that drives the level of success. The beneficial effects stemming from the supply chain allows partners to jointly gain an understanding of prospective demand and then develop realistic plans which satisfy this demand [18]. This is validated by Corbett and

Blackburn [3] who state that as partnerships between companies and suppliers mature, the competitiveness of their supply chains improve.

Supply chain management is essentially information-driven with organizations recognizing that supply chains who share information for coordinated decision-making achieve maximum efficiency for all supply chain partners. This requires supply chain partners to embrace a new philosophy based on cooperation and trust. They must seek to improve the performance of the overall system rather than individual processes or organizations within the chain. This acknowledges the new reality where competition is no longer between organizations, but between competing supply chains. Facilitating this unified approach is IT as it enables integration of information flows between partners, thus diminishing uncertainty and risk. Gunasekaran and Ngai [5] have argued that an efficient, competitive, and collaborative supply chain is impossibility without IT. Therefore, as partners deepen relationships, integrate IT systems and share greater amounts of information, increased importance must be placed on information security. However, relatively little research has been conducted in the area even though it has been suggested that supply chain information security demands significantly more attention than it is currently receiving [10,7,5].

SURVEY METHODOLOGY

While few researchers have conducted studies on information security in the context of supply chain management, Smith et al. [20] have taken steps toward identifying and framing the inherent IT security risks between collaborative partners. Their work provides the foundation for our introspective survey. Our intent is an initial investigation toward isolating, analyzing and establishing an empirical relationship between supply chain collaboration and information security risk.

The survey instrument was organized around two central themes: perceived level of information security risk and actual occurrence of security incidents. In its most basic form, risk is defined in terms of an expected value measurement. More specifically, a 'combination of probability, or frequency, of occurrence of a defined hazard and the magnitude of the consequences of the occurrence' [17]. Unfortunately, at this time, measuring supply chain information security risk is highly problematic [20]. Whereas many firms have data on security event frequencies and probabilities, the magnitude of financial impact associated with these events is not easily measurable or available. Attempts to ascertain this information often result in nothing more than mere conjecture of the likely financial impact incurred from a security event as firm's often severely overstate or understate their position. Due to these circumstances, we did not attempt to quantitatively measure risk (probability × consequences). For measurement, we asked survey participants if their organization suffered an information security incident directly related to a supply chain partner. We surmise that it is logical for firms having a higher likelihood of security incidents to have higher risk. For the purposes of this research, an anecdotal risk assessment provides a working measure.

Conducting research involving information security programs has proven to be a challenge. For obvious reasons, firms are often reluctant to divulge information about security practices and problems to outside parties. Prior research has, however, suggested that partnering with a trusted entity (i.e., government body or independent security company) when conducting information security research encourages participation and improves results [8]. To establish a trustworthy relationship, the survey discussed in this paper was developed and conducted in cooperation with Cybertrust, the world's largest information security services company. Upon completion of survey design, the authors employed a third party surveying company, retained by Cybertrust to perform industry and marketing surveys, to manage survey distribution.

Due to the nature of the survey, the authors felt that the ideal target sample was individuals with knowledge or responsibility for IT, security, and operational functions within the firm. Such individuals likely have an intimate and realistic knowledge of IT in their firms and the technological risks associated with collaboration and integration with supply chain partners. Individuals fitting this description were randomly selected from a proprietary list of firms maintained by a third-party organization and invited to participate via email. Because the survey involved highly sensitive information, it was conducted anonymously to promote trust and honest responses. As an incentive,

participants were offered a full report of results. Two rounds of follow-up emails were sent to non-respondents to further encourage participation.

In total, 206 firms completed the survey. Of those, twenty-three were eliminated from the final analysis due to non-existent or undefined supply chain relationships. The 183 remaining firms represent various supply chain functional areas ranging from manufacturing to retail. Firms of all sizes, ranging from fewer than fifty to greater than 100,000 employees, participated in the study. Respondents described their role in the firm as IT administration (38%), IT management (20%), operational management (32%) and senior management (10%). The following sections highlight noteworthy findings of the survey.

SURVEY RESULTS

Collaboration and Perception of Risk

Respondents were queried about their perceived information security risk to examine what factors and activities related to supply chain collaboration were influential. This is represents a "gut feeling" measure of risk.

When asked how collaborative activities with supply chain partners affect their firm's risk of information security incidents, nearly three-quarters of all respondents reported an increase. These results are depicted on Figure 1. Deeper analysis revealed that 73% of IT professionals, both administration and management, reported some increase, with 48% of administrators and 40% of IT managers perceiving moderate to greatly increased risk due to supply chain collaboration. Operations management respondents reported the largest proportion of some increase (75%), with 50% perceiving moderate to greatly increased risk. Interestingly, 50% of senior management responded that they perceived supply chain activities having no impact or actually decreasing the risk of information security incidents. Only 17% of senior managers responded that supply chain collaboration activities moderately to greatly increased risk. While the responses by IT and OM personnel appear to be aligned, there appears to be a disconnect between these groups and senior management.

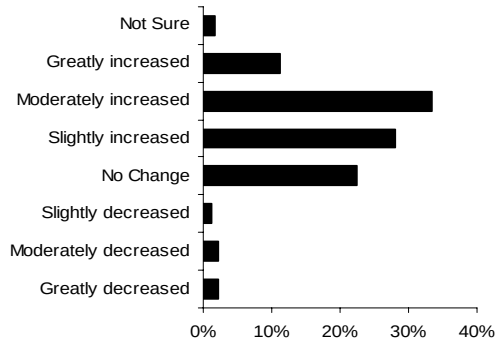

Figure 1. Perceived effect of supply chain collaboration on information security risk.

When asked to identify the most worrisome security risks stemming from supply chain partners, respondents identified network intrusions (68%), data theft (64%), virus infections (49%) and fraud/misuse (43%) most often in their responses.

Collaboration and Incident Probability

Though perceptions of risk provide valuable insight, they obviously cannot reveal factors that actually increase information security risk in collaborating firms. To assess whether perceptions of risk were founded, we asked respondents if their firm had suffered an information security incident directly involving their supply chain partners within the previous year. We were quite surprised to find that thirty-seven percent of all firms reported at least one incident. In addition, thirteen percent of the respondents have terminated at least one business partnership because of information security incidents or concerns. This offers compelling evidence that information security is a real and critical problem for supply chain management.

As follow-on, participants were asked a series of questions about the levels of their partner relationships, the amount of information exchanged, and IT integration with supply chain partners. Analysis was then conducted to determine how collaborative activities among supply chain partners affected the chance of security incidents. Figure 2 reports the findings, showing the percentage of firms reporting an incident at successive levels of each activity. An association is revealed where an increase in

collaborative practices results in a steady increase in incident probability. The notable exception to this trend is the thirty-two percent drop in incident likelihood as IT integration moves from high to very high levels. This analysis suggests that firms with very high levels of IT integration have significantly more advanced security practices in place to mitigate risks.

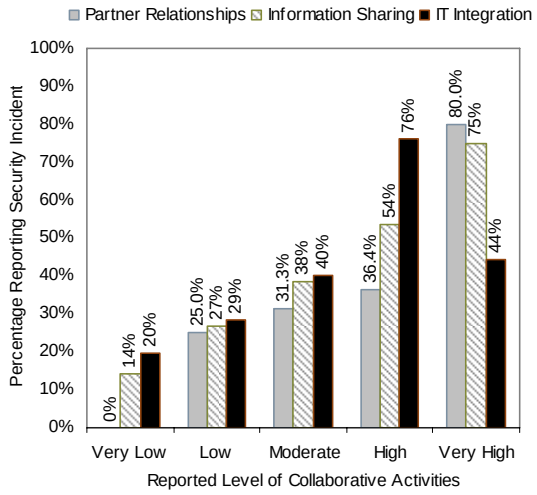

Figure 2. Effect of collaborative activities on incident probability

Mitigating Factors on Incident Probability

Conventional wisdom suggests that the potential benefits from collaboration exceed the added risks; therefore, an appropriate response to these findings does not involve cessation of supply chain collaboration. However, the association between collaboration and information security makes it imperative that those responsible for supply chain operations be aware of and take action to mitigate potential threats. We chose to examine the implementation of four measures suggested by a collaborative group of information security professionals at Cybertrust to mitigate risk within the context of interconnected IT systems. They are:

1. Practices adopted to improve the firm's IT security posture,
2. If/When assessments of a potential partner's information systems security are conducted,
3. How this assessment is conducted,
4. Management's consideration of security risks in decisions regarding supply chain partnerships.

To be sure, the list is not exhaustive but it provides ample opportunity to test whether incident probability can be controlled among collaborating firms.

Survey respondents were asked to rate their firm's level of adherence to each of these factors. When asked to rate their firm's information security practices for risk directly related to business partners, we found a fairly even distribution of practices between below average, average, and above average. However, further analysis of the data reveals a startling disparity between the perceptions of IT administrators, IT and operations managers, and senior management. Fifty percent of senior managers perceive their information security practices as either excellent or above average, this contrasts with 38 and 39% of IT and operations managers, and only 25% of IT administrators. As with the perception of risk associated with supply chain collaboration, responses point to a disconnect between those who are tasked with accomplishing strategic objectives and those who develop the objectives.

A second disparity identified in the data was based on the level of IT integration and the security practices used to mitigate information security risk. As suggested in the previous section, companies at the highest levels of IT integration appear to be aware of and better able to protect themselves from information security risks. As displayed in figure 3, when managers were asked to rate their security practices, there was little difference between those in organizations self-reporting low or moderate levels of integration. However, in organizations with high or very high levels of supply chain integration, none of the respondents reported below average practices and more than 63% reported above average or excellent information security practices. Of the firms reporting very high levels of integration, all reported above average or excellent security practices.

The question of assessing a potential partner's information systems security presented a two part challenge. First, we asked when, if ever, a potential partner's information security systems are assessed. We found that twenty-four percent of respondents assess prior to and during a

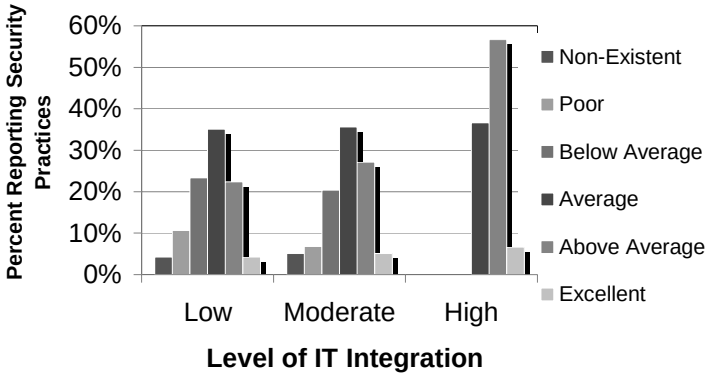

Figure 3. Perceived Level of Security Practice Based on Level of Integration

partner relationship; nineteen percent assess prior to the relationship; eight percent assess during the relationship; thirty-eight percent do not assess at all; and eleven percent are not sure if an assessment is done. Given the strategic importance of collaboration for supply chain integration, it is worrisome that 49% of respondents were either doing nothing or unaware of the actions taken to protect the firm from information security risks. This apathy toward information security in the supply chain was not limited to those with low to moderate levels of integration. While 100% of firms reporting very high integration assess partner IT security practices before establishing and during a relationship, more than 40% of those reporting high levels of integration either did not assess or did not know whether an assessment was made.

Having established when security systems were assessed, the next step was to determine how the assessment was conducted. For those who performed assessments, the results are as follows:

- 34% have a formal agreement or policy in place which mandates adherence to certain security practices,
- 15% have a formal agreement or policy in place which mandates adherence to certain security practices, plus they audit or assess their security practices in-person,
- 20% have a formal agreement or policy in place which mandates adherence to certain security practices, plus they audit or assess their security practices remotely,
- 31% have an informal agreement or policy in place where they accept the promise of their partner to do a sufficient job securing their systems.

The biggest challenge was to query each participant on their management's consideration of security risks. To this end, we gathered respondents' opinions pertaining to the level of consideration that management *should* give to potential information security risks during decisions regarding supply chain partnerships. A breakdown of responses is shown in Figure 4a. Ninety-one percent of participants felt management should give at least moderate consideration, while only five percent answered none or low. This reflects a clear understanding of an existing threat by IT, OM, and top management.

Next, participants were queried about the level of consideration *actually given* by management to these issues at their firm. The results, found in Figure 4b, display an obvious contrast between "should" and "does". Almost half (46%) of respondents believe management gives little to no consideration to information security in supply chain management. This is quite alarming as 90% of responding firms share at least moderately confidential information with their partners.

Our analysis has pointed to this disconnect between the perceptions of those in senior management positions and IT administrators, IT managers, and operations managers on a number of issues. Senior managers are much more likely to perceive less risk, or even a reduction in risk,

due to supply chain integration than the other groups surveyed. Senior managers were more also optimistic regarding the state of security practices employed by their firms than those at lower levels in organizations. One possible explanation for this disconnect is that senior management is more focused on the benefits that can be derived from collaboration while those in positions that require them to carry out the strategic plans of management are more aware of the potential dangers that these activities may pose. Senior management's focus on benefits is understandable when considering the difficulty in quantifying information security risk in the context of supply chain management. Since no established measure of risk exists, it is difficult to conduct a cost benefit analysis let alone justify greater expenditures for security practices and audits.

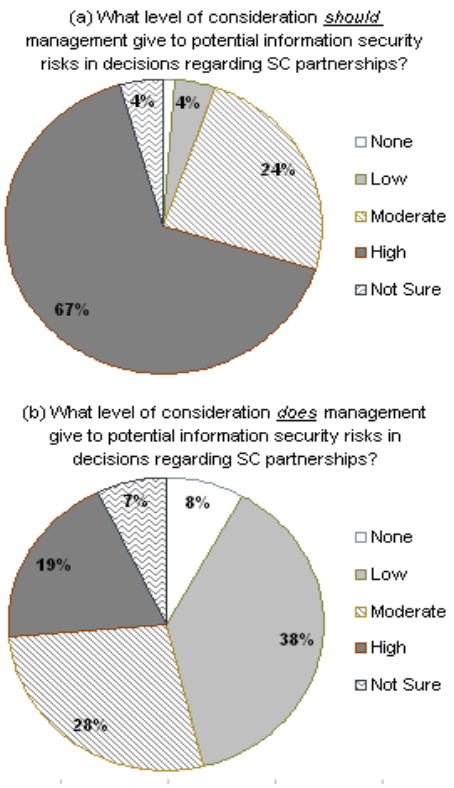

Figure 4. Comparison of opinions concerning the amount of consideration management should give information security in supply chain management and the amount actually given

CONCLUSIONS

As IT increasingly becomes the backbone of business functionality and relationships, a reliance upon its secure and continued operation has redefined corporate risk [12]. In the supply chain, collaboration is designed to drive down supply chain risk [2] through seamless integration and coordination among partners. Our study finds a strong consensus of opinion that deepening the level of the activities essential to this goal may increase risk offsetting any benefits gained. With collaboration hailed as the supply chain's most pressing need [1], this finding is disconcerting to say the least.

It appears that measures taken to improve organizational security have some ability to combat the risk of security incidents exacerbated by higher levels of collaboration. Robust IT assessments of potential partners also seem helpful in mitigating information risk. Furthermore, although our survey shows management involvement to be widely underdeveloped, those managers exhibiting high consideration of these issues may be able to garner significant benefits to their firms either in reduction of security incident related costs or in improved competitive position due to market perception of greater information security levels.

It is our intention for this brief empirical assessment of information security in supply chain management to stoke the interest of the research community while serving as a springboard for future study in the area. To be sure, collaboration introduces great benefits but at what cost? Is the more than five-fold increase in incident likelihood between information sharing extremes worth the benefits incurred? Is it possible for a firm to determine optimal levels of collaborative activities that optimize benefits while minimizing information security risks? The answer to these important questions at this time is, quite simply, more research is necessary. The importance of finding answers to these and other related questions to firms operating within today's highly interconnected, information-intensive supply chains cannot be overemphasized.

ACKNOWLEGEMENT

The authors would like to acknowledge the Cybertrust Corporation for their support of this industry survey. Cybertrust, now known as

Verizon Business Solutions, is a global provider of information security services and their continued willingness to sponsor exploratory academic and industry research is appreciated.

REFERENCES

1. Ashayeri, J. & Kampstra, R. P. (2005) Realities of Supply Chain Collaboration. *EurOMA International Conference Proceedings*. Budapest, Hungary, European Operations Management Association.
2. Christopher, M. & Peck, H. (2004) Building the Resilient Supply Chain. *International Journal of Logistics Management,* 15**,** 1.
3. Corbett, C. J. & Blackburn, J. D. (1999) Partnerships to Improve Supply Chains. (Cover story). *Sloan Management Review,* 40**,** 71.
4. Frolich, M. T. & Westbrook, R. (2001) Arcs of integration: an international study of supply chain strategies. *Journal of Operations Management,* 19**,** 185.
5. Gunasekaran, A. & Ngai, E. W. T. (2004) Information systems in supply chain integration and management. *European Journal of Operational Research,* 159**,** 269.
6. Kang, T. S. (1973) Ordinal Measures of Association and Forms of Hypotheses. *The Sociological Quarterly,* 14**,** 235-248.
7. Kolluru, R. & Meredith, P. H. (2001) Security and Trust Management in supply Chains. *Information Management & Computer Security,* 9**,** 233-236.
8. Kotulic, A. G. & Clack, J. G. (2004) Why Aren't There More Information Security Research Studies. *Information & Management,* 41**,** 597-607.
9. Lee, H. L., Padmanabhan, V. & Whang, S. (1997) Information Distortion in a Supply Chain: The Bullwhip Effect. *Management Science,* 43**,** 546.
10. Lee, H. L. & Whang, S. (2000) Information sharing in a supply chain. *International Journal of Technology Management,* 20**,** 373.
11. Li, L. (2002) Information Sharing in a Supply Chain with Horizontal Competition. *Management Science,* 48**,** 1196.
12. Loch, K. D. & Carr, H. H. (1992) Threats to information systems: Today's reality, yesterday's understanding. *MIS Quarterly,* 16**,** 173.
13. McLaren, T., Head, M. & Yuan, Y. (2002) Supply Chain Collaboration Alternatives. *Internet Research: Electronic Network Applications and Policy,* 12**,** 348-364.
14. Mentrzer, J. T. (2002) Managing Supply Chain Collaboration. *Supply Chain Management Review***,** 83.
15. Metters, R. (1997) Quantifying the bullwhip effect in supply chains. *Journal of Operations Management,* 15**,** 89.
16. Narus, J. A. & Anderson, J. C. (1996) Rethinking Distribution: Adaptive Channels. *Harvard Business Review,* 74**,** 112.
17. Pidgeon, N., Hood, C., Jones, D., Turner, B., & Gibson, R. (1992) Risk Perception. In G. Royal Society Study (Ed.), Risk: Analysis, Perception and Management. London, UK: The Royal Society.
18. Ahay, B. S. (2003) Supply Chain Collaboration: The Key to Value Creation. *Work Study,* 52**,** 76-83.
19. Simatupang, T. M. & Sridharan, R. (2005) The collaboration index: a measure for supply chain collaboration. *International Journal of Physical Distribution & Logistics Management,* 35**,** 44.
20. Smith, G. E., Watson, K. J., Baker, W. H. & Pokorski, J. (2007) A Critical Balance: Collaboration and Security in the IT-Enabled Supply Chain. *International Journal of Production Research,* 45, 11.