ABSTRACT

Information is the lifeblood of the supply chain. While the effect of information technology capability on supply chain collaboration has often been highlighted in the literature, much more remain to be understood about how information security orientation of firms can influence supply chain collaboration. Two research questions are addressed: (1) How does IT enablement affect supply chain collaboration, and (2) How does information security orientation affect the path to collaboration in IT enabled supply chains.

KEYWORDS: IT Enabled Supply Chain, Security Orientation, Collaboration

INTRODUCTION

Information is the lifeblood and is considered a key driver of supply chain performance (Chopra and Meindl, 2001). The effect of information sharing on supply chains was highlighted by different researchers like Veen-dirks and Verdaasdonk (2009) who stress how information sharing enhances inter organizational collaboration. Cultivating a collaborative environment in a supply chain allows the different partners to align their interests and values towards a unique whole (Mohr et al., 1996).

In loosely coupled supply chains characterized by less integration and less control (Malone et al., 1987), quality of shared information supported by capable information system will become crucial to its performance. The risk that information is vulnerable to threat and is not sufficiently protected against damage, modification or loss utterly hurt the supply chain performance.

Researchers continually viewed threats to information as detrimental to the whole supply chain performance. For example, Cavasuglu et al. (2002) reported that announcement of internet security breach has a negative effect on the market value of the breached firm. More specifically, they found that “breached firms, on average lose approximately 2.1% of their market values within two days surrounding the events. This translates into $ 1.65 billion average loss in market capitalization per incident.” Financial losses due to information security threats is burgeoning. For example, Whitman (2003) mentioned that financial losses due to information security threats were nearly $456 million in 2003 as compared to $78 million in 2001. Furthermore, Mcwrath (2006) found that two to three percent of an organization’s annual profit may be lost due to
information security incidents. Cisco, in their 2013 annual security report, addressed how cyber security threats might create disruptions that negatively influence supply chain performance if not managed properly. Threat severity might be devastating to the firms to a degree that diminishes the economic benefit of the information technology, as stated John Stewart the vice president of Cisco.

Risk attributed of information security breaches drives organizations to take preventive information security measures to avoid any system risk. Within the supply chain context, willingness to share information among the different partners and the level of information sharing will vary depending on information security orientation adopted (Huang and Behara, 2013). As a matter of fact, the importance of information security orientation within the today’s global supply chain supported by the information and communication technology which made make information access prevalent and consequently a highly vulnerable asset that must be secured. In this research, we study the IT enabled supply chains from a perspective that emphasizes information security as a driver of information sharing. More specifically, attempt to answer three primary questions:

**RQ1:** How does information technology capability affect supply chain collaboration?

**RQ2:** How does quality of shared information affect the relationship between information technology capability and the performance of the supply chain?

**RQ3:** What effect does information security orientation have on this relationship?

The paper is organized as follows. The first part covers the literature review and the theoretical background that we started by the brief review of resource based view related to IT and supply chain management. Then, the effect of IT on information sharing and supply chain performance is highlighted. In the second part, the research model will be explained. The third and final part shows the research methodology and how analysis could be approached.

**LITERATURE REVIEW**

**Resource Based View of the Firms (RBV)**

Wu et al. (2006) stressed how improvement in supply chain capabilities through IT allows firms to learn and respond to market changes better and quicker than competitors. According to the resource based theory of the firm, the possession of resources will not create a business value. Rather, rational deployment and integration of resources in a way that create business value is what will form a competitive advantage (Powell and Dent-Micallef, 1997). At the supply chain level, collaborative planning, forecasting and implementation supported by the exchange of quality information in a secure environment is what creates a valuable, rare, valuable, and inimitable collaborative advantage that differentiates one supply chain from the other. Secured IT is regarded as a powerful resource that helps buyers and suppliers establish the link to communicate and to exchange accurate information in a timely manner which in turn helps building trust and reliability perception in the buyer-supplier relationship. This of course will assists successful collaborative activities.
IT Enabled Supply Chains

Prior study in information research provides insight on how IT enables both inter and intra organizational collaboration (Reed and DeFillipi, 1990) leading to the success of supply chain management. Based on the RBV perspective, the capability of transferring quality information shielded with security is in itself an indispensable organizational competence necessary for innovation and continuous improvement (Barney, 1991; Duncan, 1995). Increasing the flow of information allows firms to timely solve problems (Rogers et al., 1993), and accordingly provide better performance outcomes (Bowersox et al., 1999). The firm’s capability to receive and send accurate, timely and secured information promotes better coordination, integration, communication, and interorganizational collaboration (Zhang and Dawes, 2006). It is our contention that supply chain capability can be achieved through the collaborative competence supported by information technology capability which allows quality of information sharing in an information secure environment.

Drawing from previous research that defined IT capability as a combination of both skilled workers and the technology shielded with financial support (Bhardawaj, 2000; Rai et al., 2012), the current study identifies IT capability in terms of IT human resource, IT investments, and IT policies and standards.

**IT Human Resource.** The knowledge and skills possessed by IT personnel is an important dimension of the capability of the ITI (Fink and Nuemann, 2009). In addition to being a major organization resource that supports the integration of the different functions within the organization (Broadbent and Weill 1997), human resource dimension has long been identified in the literature as crucial for the use and management of the technology (Broadbent and Weill, 1997; Duncan, 1995; Bhardwaj, 2000; Byrd, 2000). Lack of skilled IT personnel can lead to technical and operational problems that inhibit sharing of timely, accurate and relevant information through IT infrastructure.

**IT Investments.** Investment in IT infrastructure is considered a major constituent that affects all other components of ITI (Byrd et al., 2008). Investment in ITI is mandatory to all IT projects, system maintenance and upgrading, and employees training. Organizations lacking that financial flexibility may not be able to provide scheduled system maintenance which in turn negatively affect the flow of information and communication among the different supply chain entities starting from suppliers all the way to the customers. Another drawback of the insufficient investment in IT is the inability of the firm neither to hire skillful IT employees nor to provide the necessary training. This in turn will hinder benefitting from the technology within hand and will lead to improper functionality of the information system as a whole.

**IT Policies and Standards.** Policies and standards that guide the use of the information technology both internally and externally come at the heart of the information technology infrastructure. Establishing the appropriate set of clear and communicatable policies and standards allows firms to share information internally within firms and externally across firms in a more structured and straightforward way (Bhatt et al., 2010).

IT is increasingly viewed as a capability that allows firms to cope with environmental uncertainties through better coordination, integration, communication, and interorganizational collaboration (Zhang and Dawes, 2006). According to Clemons and Row (1993), IT enhances coordination within supply chains and enables transaction cost reduction among the different
partners. Information sharing capability and communication capability within supply chains allow for realistic and efficient involvement of the different partners. This is highly exemplified in companies that apply Just In Time (JIT) practices such as Dell that achieved more cost saving than any of its competitors thanks to its outstanding IT capability that allows both integration and coordination within its supply chain in a timely fashion. This, in turn, leads to faster response for customer varying needs and better coping with the environmental changes (Frohlich, 2002).

Within the intra-organizational domain, IT capability is more directed towards organizational members’ utilization and familiarity in operating IT applications. However, IT capability within the inter-organizational context accentuates the technical ability that allows integrating shared information from heterogeneous information systems adopted by other supply chain partners.

**Information Sharing and Supply Chain Collaboration**

Creating unique capabilities within supply chains requires firms to collaborate in order to benefit from the knowledge, and resources that reside outside their own boundaries. Fawcett et al. (2012, p. 60) stated that "Companies that have learned to collaborate thus find that they possess a rare and valuable capability that competitors cannot easily replicate."

As a matter of fact, supply chain collaboration has been conceptualized in different ways. Hammer (2001) regarded collaboration as a joint effort to restructure supply chain operations. Simatupang and Sridharan, (2002) defined collaboration as two or more independent companies working together to create higher levels of performance than when acting alone. Hardy et al., (2005) defined collaboration as “cooperative, inter-organizational action that produces innovative, synergistic solutions and balances divergent stakeholder concerns.” Many firms might resist collaboration opportunities because of the relational risks exemplified by security breaches, lack of commitment from the different partners, possible opportunistic behavior, appropriating partners’ resources, and distorting information, and delivering unsatisfactory products and services (Das and Teng, 1999).

Cultivating a collaborative environment mandates deploying IT capability as well as a significant level of trust. Trust among the supply chain members can be promoted through securing the information flow along the supply chain such that transparency, reliability and accountability of information transferred will form a motive force for trust. Securing the information flow will support various practices performed by the supply chain members who will become more willing to send and receive information and to interact among one another. Information security orientation of the firm will create a supportive atmosphere for trust and will act as a governance mechanism for releasing and receiving information in a timely manner. As such it is our contention that IT capability together with information security orientation within the supply chain will lay the ground for collaboration.

Nyaga (2010) proved that the collaborative information sharing, joint efforts and investments lead to trust and commitments among supply chain members. Cao and Zhang (2011) identified supply chain collaboration using information sharing, goal congruence, decision synchronization, incentive alignment, resource sharing, communication and joint knowledge creation. For the purpose of this study which explores the effect of information security orientation, and IT capability on supply chain collaboration, we define supply chain collaboration as the joint efforts among supply chain partners to co-create and deliver value that each partner cannot deliver on its own. Supply chain collaboration is viewed as a second order construct which consists of joint decision making among supply chain members which will be supported by superior
communication platforms to facilitate coordination and participation needed for collaboration among supply chain members and that will be provided through capable ITI, trust among partners because it represents an essential social element required to achieve successful collaboration and that will be strongly enhanced through sharing of accurate, relevant, timely, and recent information shielded by supply chain security orientation.

Generally speaking, information shared among supply chain members can take any of three main forms: the first is transactional information such as order quantities, prices, sales, product specifications, quality, and delivery specifications; the second is operational information such as inventory levels, costs and schedules, production and transportation capacities, lead times, and shipments; and the third, strategic information such as aggregated point-of-sale information, demand, market trends, and product design (Yang and Maxwell, 2011). It is our contention that sharing of quality information among supply chain partners positively influence the joint decision making process across the supply chain which in turn permits policy makers and practitioners to proceed with greater confidence in their outcomes.

As a matter of fact, the positive effect of information sharing on collaborative advantage within supply chain context was intensively discussed decades ago. For example, Stein and Sweat (1998) found that supply chains that collaborate through sharing information on a regular base are more capable of responding to customer needs and coping with market behavior. Literature confirms that sharing information within a supply chain can substantially reduce information distortion contributing to “the bullwhip effect” which eventually leads to improved performance of the supply chain as a whole (Lee et al., 1997; Wu et al., 2014). Let us recall that information is a major performance driver of any supply chain as discussed by Chopra and Meindle (2001). An in-depth look at Chopra and Meindle’s conceptualization of supply chain performance reveals how information is necessary for coordinating decisions related to location selection, inventory strategies, production scheduling, selecting the best mode of transportation, evaluating supplier among many other decisions that lead to lowering the total supply chain cost, increasing the order fulfillment rate and reducing the order cycle time (Lin et al., 2002). Researchers contend that in order for information to enhance a collaborative advantage of a supply chain, it needs to be accurate, relevant, and timely together with the representational quality to make it easy to understand, interpret and manipulate (Lee et al., 2002). Increasing the information quality increases the value that can be created from information and hence increases the chances of collaboration success. Li et al. (2006) discussed supply chain from the viewpoint of “buyer-supplier relationship” and they reported that communicating information about demand, for example, with certain level of quality (accuracy, time) will largely reduce bullwhip effect resulting in reduced level of uncertainty and disruptions.

In collaborative supply chains, information sharing is expected to take place at interpersonal, intra-organizational, and inter-organizational levels. In organizational behavior literature, interpersonal level of information sharing was studied based on both the personal behavior towards sharing information (Jarvenpaa and Staples, 2001), and the motives behind people who are willing to share information with others (Marshall and Bly, 2004). Specifically, Marshall and Bly viewed information sharing as a behavior that can be operationalized to establish strong social ties between receivers and senders of information. In a one to one analogy, receivers and senders can be represented by the buyer-supplier relationship in the supply chain context. Intra-organizational information sharing literature was directed towards building organizational capabilities necessary for problem solving and organizational knowledge creation (i.e Ardichvill et al., 2003; Cress and Kimmerle, 2006). Viewed from the inter-organizational perspective,
information sharing is an enhancer for the establishing a collaborative advantage among the supply chain partners (Yang and Maxwell, 2011).

Socio-technical aspects necessary for sharing information were investigated by Wu et al. (2014) who studied how social aspects affect the information sharing within and across organizations. They found that trust, commitment, and reciprocity are all necessary for building a collaborative supply chain through information sharing among the various partners. Collaboration will form the “non-contractual” tool for solving problems that might arise over time. The social aspect will be emphasized through the willingness of each party to exchange information in a way that allows the collaborative supply chain relationships and activities to adopt over time and creates new avenues for more collaboration and joint decision making (Nyaga et al., 2010).

**Information Security Orientation**

In today’s globally interconnected supply chains, with increasing reliance on information technology to achieve competitive advantage, information security is and has been by far one of the most important yet crucial requirement for supply chains success. It is clear now how information is a critical resource for supply chain success. Information sharing motivates willingness to engage in collaborative activities among the supply chain partners (Nyaga et al. 2010; Wu et al. 2014). Information should be shared among supply chain partners with high level of confidentiality, integrity, and availability of data (Zafar, 2013). Building a security orientation among supply chain members is necessary to avoid: (1) unrecoverable destruction of the information asset, (2) unauthorized access and /or modification to the information, (3) disclosure through uncontrolled access or release of information; and (4) denial of services which causes information system to be unavailable to authorized users to retrieve desired information (Wilson et al., 1992).

Due to the socio-technical nature of information technology (Orlikowski, 1992; Orlikowski, 1992; Colombo and Delmastro, 2002), we believe that information can be threatened due to either technical and/or behavioral breaches. Threats that occur at the technical level can be viewed from four broad scopes: software, hardware, networking, and data. Threats at this level can be caused by unplanned modifications, destruction, unintentional loss, theft, interception, interruption and can be controlled through technical measures. At the behavior level, Waxer (2007) referred to three main behavioral related threats: (1) employees unintentionally giving out the company information, (2) employees losing their devices, and (3) spreading information through unsecured emails. Enforcing an information security will most probably reduce information security breaches and will positively influence the functioning of the different firms. Siponen (2001) clearly stated that "A company with gaps (mostly unplanned) in its culture on information security issues will most probably have Information Security (ISEC) breaches, which will have significant influences on the functions of the company. Thus, the employees have to take their responsibility for the company’s ISEC."

Nurturing an information security orientation at the supply chain level is an important step towards building a “collaborative we” environment (Kanter, 2000). This can be interpreted through the threat-rigidity theory that posits that an individual will have a maladaptive response to collaborative efforts if they feel some sort of threat (Moon and Conlon, 2002). Potential threatening events produce rigidity and unwillingness to share information among the partners. On the other hand, the confidence an individual have towards the information technology adopted by the different actors will encourage more information sharing and more collaboration.
HYPOTHESES DEVELOPMENT

Based on the integrated viewpoint of the literature stream reviewed, we found that the theoretical model presented in Figure 1 might best describe the link between IT capability that many firms have embraced across the globe and supply chain collaboration. Further, the model focuses on key elements of this relationship such as: (1) the mediating effect of information related characteristics such as relevancy, accuracy and timeliness that we referred to as quality of shared information, and (2) the moderating effect of information security orientation adopted by supply chain members.

The Effect of IT Capability on Supply Chain Collaboration

Supply chain collaboration is often defined as “two or more chain members working together to create a competitive advantage through sharing information, making joint decisions, and sharing benefits which result from greater profitability of satisfying end customer needs than acting alone” (Simatupang & Sridharan, 2005; Whipple & Russell, 2007). Although the number of “potential” collaboration benefits cited in the literature outnumber its counterpart “potential” risks, several authors have indicated that efforts to collaborate between firms is not always successful (Simatupang & Sridharan, 2002; Whipple, 2007). This can be referred to the fear that companies experience if information sharing was not shielded by security.

Byrd et al. (2008) stated that capable IT infrastructure is the foundation to deliver quality information that is accurate, timely, relevant, reliable, and complete. Past literature has also suggested that quality of shared information has the potential to reduce uncertainty which in turn boosts trust and commitment to the relationship among the supply chain partners (Kwon and Suh, 2004; Nyaga, 2010). IT also supports efficient communication and collaboration among the different entities within a supply chain through facilitating joint planning and execution of different supply chain operations (Simatupang and Sridharan, 2002). This of course can potentially reduce conflict among the different partners who become better able to share relevant, complete, and consistent information among each other more comfortably in a timely manner (Kumar and Van Diesel, 1996). In addition, quality of shared information can also reduce uncertainty which in turn boosts trust and commitment to the relationship among the supply chain partners (Kwon and Suh, 2004; Nyaga, 2010). Although Cao and Zhang (2011) identified supply chain collaboration using different measures among which is information sharing, we embrace a different opinion that entails that in order to build a supply chain collaboration, and quality of shared information should be present in the first place in order for collaboration to take place. Therefore we posit that:

H1: IT capability will positively influence supply chain collaboration.

H2: Quality of shared information is positively associated with supply chain collaboration (is an antecedent to supply chain collaboration).
Researchers within the IT literature have considered IT as a significant enabler for information sharing within supply chains (Magretta, 1998; Reda, 1999; Li et al. 2006; Li and Lin, 2006). Capable IT infrastructure will support sharing of critical and proprietary information among the supply chain partners (Li and Lin, 2006). Shared information can vary from strategic to tactical and from general information about logistics activities and general markets to highly specialized information about customers and suppliers (Li et al., 2005). Capable ITI consists of various components that Byrd and Turner (2001) grouped as: technology which includes software, hardware, services, and network that Ray et al. (2005) called it “generic technology”; IT human resource, IT investments, and ITI policies and standards. The use of such technology facilitated efficient information sharing within the supply chain and helped in building effective way of
communications among the different supply chain entities. For example, Weill and Broadbent (1998) indicated how IT forms the basis that supports various business applications and services within organizations. Reda (1999) showed how ITI enables faster transfer of information to business partners, and Frohlich (2002) alleged how web-based technology allowed information sharing within the buyer-supplier context. In order for ITI to form a capability, it needs to be complemented with other firm resource. That line of thinking that just considers the generic technology as ITI will not be sufficient any more (Bhardwaj, 2000; Liu et al., 2013). Capability of ITI that is based on the complimentarily of the technology with firm resources is what creates the real value for the ITI and eventually the competitive advantage. In that sense, we decided to group IT human resource, IT investments, and ITI policies and standards together with the generic technology to form the information technology infrastructure capability construct.

In order for information to enhance the performance of a supply chain, it needs to be with a certain level of accuracy, relevancy, and timeliness. Impact of information sharing depends on what information is shared, with what level of accuracy, at what time, and with whom (Chizzo, 1998). Lee et al. (2002) comprehensively covered the information quality dimensions literature that they grouped into four main categories: “Intrinsic IQ, contextual IQ, representational IQ, and accessibility IQ” Intrinsic IQ implies that information has quality in its own right. Contextual IQ highlights how information must be “relevant, timely, complete, and appropriate in terms of amount” to add value within a specified context. Representational IQ addresses the degree to which information is “interpretable, easy to understand, easy to manipulate, and is represented concisely and consistently. Accessibility IQ emphasizes the ease with which information can be accessed and accessed.”

**H3:** IT capability positively influence quality of shared information within a supply chain.

**The Moderating Effect of Information Security Orientation**

Although technical security control is thought to increase the level of protection of information, it is not sufficient in itself to ensure system security. Rather, a security pyramid that includes three main levels of security control was suggested in the literature. The security pyramids has technical security at its base and on the top of it comes the formal security that can be established through policies, procedures and guidelines, and finally comes informal security at the top of the pyramids and it can be established through embedding the security concept within the organization culture. It is needed to show how each level of security control affects the relationship between IT and level of supply chain information sharing. In our analysis we differentiate between two complementary groups of measures to ensure information security. The first is a group of technical measures to protect the hardware, software and data from being modified, disclosed, intercepted, destroyed, interrupted, or fabricated (Dhillon, 2001); and the second group includes administrative measures like policies, procedures, guidelines as well as security culture building activities in terms of training and awareness programs (Dhillon, 2006).

It is our contention that security measures at the technical level will reduce system disturbance and will guarantee smoother flow of information. In addition, having such measures in place will intrinsically motivate employees to avoid “insecure practices” that might expose them and their organizations to different kinds of problems (Stewart, 2004, Thomson and Solms, 2005, Chai et al., 2006). Furthermore, security measures and enforcement of security culture will improve the image of the firm in the eyes of the suppliers and customers through the trust they will have
about the system and the comfort they will get regarding sharing information. This of course will result in attracting other supply chain partners to share information among each other without any fear of undesirable consequences that might have occurred in case of absence of such measures.

Administrative security measures can be broadly divided into “formal” and “informal” security measures (Dhillon, 2006). Formal measures set policies, procedures, rules, and guidelines needed to create the environment for technical control to be effectively implemented across the organization (Dhillon, 2006). Security policies help in managing information sharing through setting the minimum security roles, responsibilities, authorized use of information, prohibited uses, and requirements for security management (Whitman and Mattords, 2008). For that reason, we believe that law enforcement and accountability established by such policies and regulations within each organization and among the different organizations within a supply chain will positively influence the quality of shared information since accountability will be enforced for information sent and received. This in turn will reduce any ambiguity and will lay the ground for transparency among the different entities within the supply chain. Clarity of the formal measure will facilitate implementation and will reduce friction within the supply chain (Anderson, 2007).

Informal measures that consist of training, awareness programs and other culture building activities are necessary to shape employee behavior related to information security and privacy (Finne, 1996; Dhillon, 2006). Dhillon (2006) identified informal security control as “a subculture where meanings are established, intentions are understood, beliefs are formed, and commitments and responsibilities are made, altered, and discharged” (Dhillon, 2006: p. 4). Through this lens, we can argue that building an inter-organizational security culture will open lines of communication and remove barriers between supply chain partners which, in turn, enhance opinion convergence through facilitating information exchange (Baskerville, 1991). As a result, better relationship will be attained between the different members in such a way that allows information providers and recipients to trust each other (Li and Lin, 2006). In addition, security training programs will increase the awareness level among the different parties as well as the different individuals, and will motivate them towards security behavior. Therefore, shared vision, high collaboration and higher level of information sharing could be realized within the supply chain.

After all, it is the security measures that drive how ITI capability will be deployed toward sharing quality information. If the moderating effects of security measures are not taken into account, the impact of explicit resources (technical IT skills, generic information technologies, and IT spending) on information sharing may be veiled. Therefore, It is hypothesized that:

**H4a:** Information security orientation moderates the relationship between IT capability and quality of shared information.

**H4b:** Information security orientation moderates the relationship between IT capability and supply chain collaboration.

**RESEARCH METHODOLOGY**

This section is intended to describe the research methodology that will be deployed to test the research model in Figure1.
Sampling

A sampling frame of 800 companies will be randomly drawn from a population of 2500 publicly traded firms that are identified in COMPUSTAT as having a strong information system with different specialization. Although a sample size of 385 respondents will be needed to achieve a 95% confidence level, 0.5 standard deviation, and a margin of error (confidence interval) of +/- 5%, we will send the survey to 800 companies to increase the chance of getting the appropriate number of completed survey from busy managers where some of them might not have any time to respond to the survey question. In other words, we will attempt to contact higher number of respondents than what really needed to avoid getting very low number of completed survey that might not be enough for statistical analysis. For each company, the survey will be mailed to IT managers, supply chain managers, plant managers, and logistics managers who are knowledgeable about the use of IT enablers (i.e., electronic data interchange, internet, etc.) in sharing trade, proprietary and core business information within and across firms.

A descriptive statistics of the contacted companies as well as the respondents will be provided for those who completed the survey and those who did not complete the survey in order to be able to build better inferences and conclusion based on our analysis. For example, statistics about sales revenue, number of employees, type of industry as well as the position of respondents will be provided.

Instrument

For all our constructs, we will be using scales developed in the literature except for the security orientation construct for which we will develop a scale and validate it according to Heeler and Ray (1972) to assess the level information security within the organization. For all our survey items, we will try to have specific and focused questions that are closed ended to encourage each respondent to answer, in an attempt to increase the response rate and the reliability of the results.

MEASUREMENT ASSESSMENT

Testing for non-response bias

To detect nonresponse bias, variables will be tested for differences between early respondents and late respondents. A random sample of 10% will be taken from each of the early and late respondent groups. Group comparison will be carried out using a random selection of the variables in each of the constructs. Then t-test will be used to compare the sample means for each of the variables across groups.

Content validity

Content validity depends on how well the researchers create measurement items to cover the domain of the variable being measured (Nunnally, 1978). Content validity is a rational judgmental process that does not depend on any numerical analysis. Instead, an intensive review of literature to be able to identify the measurement items for the different constructs of the model to assure the appropriateness and completeness of items that needed to be measured.

Unidimensionality
Unidimensionality can be tested using multiple fit criteria. Two goodness of fit can be used: GFI and RMR. GFI values of 0.90 and higher, or RMR values of 0.05 or lower suggest no evidence of a lack of unidimensionality (Li et al. 2005).

**Discriminant validity**

Li et al. (2005) referred to discriminant validity as “the uniqueness and the independence of the measures, i.e., the extent to which the measures are distinctly different from each other”. To test the research model for discriminant validity, we need to consider two constructs at a time. If the hypothesis that the two constructs together form a single construct is rejected, then the two constructs are distinct from each other, and the discriminant validity holds.

**Reliability and Validity**

A pilot test of the measurement instrument will be performed with a panel of academicians and industry experts. Once feedback from the panel is obtained, the measurement items will be refined and improved. The pilot test and the feedback from the panel will contribute to enhanced content validity.

After collecting the data, the measurement items for each construct will be analyzed through the continuous improvement cycle according to Chen and Paulraj (2004). In the first stage, internal consistency will be assured through three main steps following Flynn et al. (1994). First constructs will be accepted if the Cronbach’s alpha value is greater than 0.7. For values with Cronbach of at least 0.6, constructs will be evaluated for possible improvement. Constructs with Cronbach of less than 0.6 will be eliminated. The second stage involves exploratory factor analysis. Items that do not load high on the factor they intended to measure will be deleted from consideration. The last stage involves confirmatory factor analysis. Measurement models ($R^2$) less than .30 will be discarded.

**HYPOTHESIS TESTING**

The unit of analysis will be the supply chain dyadic relationship between a manufacturing firm and an associated supplier. The hypotheses will be tested using structural equation modeling.

**DISCUSSION AND CONCLUSION**

Researchers within the IT literature have considered IT as a significant enabler for information sharing within the supply chain (Magretta, 1998; Li et al., 2006; Li and Lin, 2006). Supply chain competency can be increased through quality of shared information. For example, the quality of shared information regarding inventory level, material availability, supplier performance, and different departmental performance within each factory tend to enhance the operational competency (Ravichandran and Lertwongsatien 2005, Li et al. 2005). Quality of shared information enables accurate decision making among supply chain partners among supply chain partners (Bhatt et al. 2010). In order for supply chain partners to benefit from the information, information has to be accurate, complete in the sense that it provides all the necessary information, available on a timely manner, current and in an appropriate format (Mohr and Sohi, 1995; Wixcom and Todd, 2005; Setia et al., 2013). In other words, information should
meet certain quality criteria to be efficiently and effectively deployed and to increase the performance of supply chain (Shore and Venkatachalam, 2003).

It is our contention in this study that the quality of shared information will promote trust among the supply chain partners and it will enable the synchronization of decisions. Quality of shared information allows firms to understand supply chain dynamics more quickly and to promptly develop better mechanisms to deal with these changes. This of course will lead to better collaboration among the supply chain partners. We expect information security culture to positively moderate the relationship between IT capability and the quality of shared information. At higher level of security orientation, the influence of information technology on quality of shared information will be stronger. This of course will be largely due to the reduced downtime and reduced risk of security breaches. In addition, we posit that at higher level of security orientation the direct effect of IT capability on collaboration among supply chain members will be stronger. The reason behind that is security orientation will create an atmosphere of comfort among the supply chain members to share proprietary information without having a doubt that the information might be leaked, altered or damaged. We believe that accountability established by such security orientation within each organization and among the different organizations within a supply chain will positively influence the quality of shared information since responsibility of information sent and received will be established.

REFERENCES


