Review Paper

INFORMATION SECURITY RISKS IN SUPPLY CHAIN MANAGEMENT: A REVIEW OF LITERATURE FOR THE DEVELOPING COUNTRY CONTEXT

Irfan Ulhaq
RMIT University Vietnam
irfan.ulhaq@rmit.edu.vn

Kevin Titus Kuruvilla
RMIT University Vietnam
kevin.kuruvilla@rmit.edu.vn

Mathews Nkhoma
RMIT University Vietnam
mathews nkhoma@rmit.edu.vn

Hanh Hong Vu
RMIT University Vietnam
hanh.vuhong@rmit.edu.vn

Ngan Truong Tuyet
RMIT University Vietnam
ngan.truongthituyet@rmit.edu.vn

Abstract

The security of information is up most important for not only organisations but also their supply chains. Based on literature review, the study proposes a framework implementing information protection that supports supply chain management at intra-organisational and inter-organisational levels in the developing country context. The paper suggests that developing countries’ dimensions of power distance, uncertainty avoidance, and collectivism actively support information protection practices in supply chain management.

Key Terms: information security, supply chain management, information risk management, intra and inter security protection

1. Introduction

Increasingly, information security in SCM has raised a controversial topic among scholars and practitioners. Together with the development of Information Technology (IT), the cooperative performance of organisations has been enhanced by the agile, diffusion, and openness of information sharing practices amongst them (Sindhija & Kunnathur 2015; Smith et al. 2007). Nevertheless, better interconnection does not come without risks. Modern IT has eliminated security barriers around resources and systems thus, given supply chains more opportunities to achieve better profitability and customer satisfaction by reducing production and inventory wastes (Svensson 2002) while on the contrary, put them into a higher possibility of disruption (Smith et al. 2007; Bandyopadhyay et al. 2010; Kerschbaum et al. 2011). An organisation loses private information related to its supply chain can negatively impact future contractual decisions of its partners. This also poses serious threats to losing business and future partnerships with potential suppliers. In fact, a great number of firms have tried to cut the
Supplementing the human aspect of information security, scholars have been interested in the idea that information protection should be applied at both technical and human components of information security risks. However, in many cases, they are still reluctant to process information within their supply chain due to the fear of information security attacks from malicious individuals or groups (Zhang & Li 2006).

Supply chains and information security have been an interest in the literature for decades. Nevertheless, scholars have been mainly paid attention on technical controls to information protection. They introduced solutions in the shapes of tools that maintain the flows of high quality data ensure the smoothness and safety of information integration, improve firewalls, and a great number of other comparable resolutions. Little attention, on the contrary, has been paid to the human aspect of information security. It is obvious that human intentions come from both internal and external organisations are sources of security problems including data theft, hacking, and invasions of users’ privacy. The significant rise of information security risks despite sophisticated technical controls today persuade us to believe that the most advanced technologies are still insufficient to a totally secured system.

On the other hand, early literature on information security in supply chains was mostly conducted in industrialised countries. Later on, globalisation broadens the framework of business to the rest of the world that calls for research at a wider scope. Indeed, there have been studies on global supply chain management yet only a few of them consider the disparity of cultural factors. This, as a result, creates a gap between supply chain information security in literature and that in practices. This paper, hence, focuses on supply chain information security in developing countries, including different facets of information security management.

2. Understanding Information Security Risks in Supply Chain Management

In general, information security risks are defined as the loss or degradation of any of the primary security goals: confidentiality, integrity, and availability of information (Smith et al. 2007; Chellappa & Pavlou 2002; Gordon & Loeb 2002). Confidentiality restricts access to private and secret information to authorised users. Integrity prevents unauthorised users from altering the information. Availability ensures the information is available when it is needed. The risks of losing these values can occur due to direct or inadvertent actions yet they cause the same consequences ranging from inconvenient to catastrophic (Smith et al. 2007). The disclosure of confidential information to unauthorised parties may damage partners’ strategies and competitiveness (Li & Zhang 2008). Improper modification and unreliable information possibly result in disturbance for the manufacturing processes which leads to bullwhip (Svensson 2002; Gordon & Loeb 2002). Moreover, the information transferring amongst partners can be interrupted or inaccessible due to losses of IT asset availabilities which eventually affects the decision-making processes of parties (Gustin et al. 1995).

According to (Smith et al. 2007; Williams et al. 2008), information security risks of a supply chain should be managed in both internal (i.e. intra-organisational) and external (i.e. inter-organisational) environments. (M. Voss et al. 2009) suggested that a supply chain in which partners take care of not only their own internal security measures but also other trading partners would have a greater ability to recognise and recuperate from security incidents both within their own organisations and across the supply chain. Similarly, (Yang & Wei 2013) also concurs the idea that information security management and partnership management are essential elements of an effective supply chain. On the other hand, there has been scholars suggest that information protection should be applied at both technical and human components. According to (Dhillon & Backhouse 2000), information management in organisations contains three aspects, i.e. technical (addressing automated components of the system such as computers, data networks), formal (addressing protection mechanisms at organisational level including policies, strategies, and standardised procedures), and informal (addressing security at an individual level such as developing shared values and beliefs, encouraging appropriate attitudes towards information protection). At an inter-organisational
level, researchers emphasised the importance of collaboration within and without the scope of supply chains (Stevens 1989). (Wunram, Weber, Pawar 2002) concurs the idea that organisations should define shared targets, strategies, procedures, and technical tools that allow them to improve the security of information systems while encouraging employees generating and sharing knowledge. This paper, hence, employs the idea of managing information security internally and externally with different perspectives to both technical and human components.

**Key:**
- P1a: Anderson (1972); Dhillon & Backhouse (2000); Faisal et al. (2006); Gordon & Loeb (2002); Sandhu et al. (1995)
- P1b: Thomson & Solms (1998)
- P1c: Safa & Von Solms (2016); Lin 2007; Tamjidyamcholo et al. 2014
- P2a: Jonscher & Dittrich (1994); Zeng et al. (2012)
- P2b: Smith et al. (2007); M. Voss et al. (2009)
- P2c: Schechter & Smith (2003); Zhao & White (2012)
3. The Developing Country Context

(Dickson et al. 2003) implies that management practices are influenced by cultural factors, thus, vary among different cultures. It is, hence, essential that scholars understand key elements defining the developing country context. Greet Hofstede is a leading culture researcher that introduced a set of dimensions to measure cultures. By implementing his study, most developing countries are characterised as being high in power distance and uncertainty avoidance, and low in individualism (Cusworth & Franks 2014; Al-Suqri et al. 2013). Power distance represents the degree to which less powerful people approve and expect the inequality of power distribution (Hofstede et al. 2010). In a high power distance culture, people tend to appreciate dominant management behaviours. Leaders are supposed to give orders and subordinates are supposed to follow their decisions without questioning. Uncertainty avoidance measure how comfortable or uncomfortable a society is in unstructured situations, e.g. unknown, surprising future (Hofstede et al. 2010). Uncertainty avoiding cultures try to minimise such circumstance by putting efforts into protection and security. Individualism, on the other hand, expresses the extent to which individuals integrate into groups (Hofstede et al. 2010). People in cultures that are low individualistic, also called collectivistic, put the good of society before that of themselves.

4. Information Security Implementation at Intra-organizational Level

Many scholars have relied on technical controls to manage information security in intra-organizational context (Dhillon & Backhouse 2000; Sandhu et al. 1995; Anderson 1972; Gordon & Loeb 2002; Faisal et al. 2006). They argued that information communicated by a company to its supply chain is mostly critical yet vulnerable that requires protection at an internal level (Faisal et al. 2006). The technical control mechanisms can mostly be implemented through the use of Enterprise Resource Planning (ERP) software. Nevertheless, there has been research indicated that an organization must not wholly rely on ERP in terms of technical knowledge coordination between the different entities (Koh et al, 2006). In conjunction with any ERP implementation, the use of a knowledge management system can help reduce some of the unforeseen issues that may arise in the supply chain (Koh and Gunasekaran, 2006). There have also been studies (Dynes et al. 2005; Kumar and Tidas 2006) reinforced the link between the availability of an information infrastructure to the associated risks that may affect business units within an organization. Surveys have also confirmed that most security breaches in any organizations have been connected to internal employees' actions rather than external entities (Baker et al., 2010; Richardson, 2011) which, in turn, is result in the need for a comprehensive security policy to prevent such actions. And while the technical aspects of any security policy form the basis of the security infrastructure in any organization, they need to be examined in totality with the people and the business process they are interlinked with (Herath and Rao, 2009).

Technical controls are classified tools implemented to help organizations protect hardware, software and data from being stolen, modified, disclosed, interrupted or destroyed (Dhillon & Backhouse 2000). The very basic technical tools have been widely used, such as anti-virus software, encryption, firewalls, digital signature and certificates, intrusion detection/protection system, in most of the organizations when speaking about enterprise security (Zafar & Clark 2009; Mejias 2012; Shaw et al. 2009; Ifinedo 2012; Tamjidyamcholo et al. 2014). Besides, technical controls also include access control mechanisms, which are biometric identification and password control, that only allow the access of authorised users to a computer system (Sindhuja & Kunnathur 2015). The access control mechanisms need to be checked against the control procedures which are used to evaluate user queries against set authorization rules in the organization (E.Y. Li et al, 2007). There also been research that have identified 2 main types of access control as role base access control and predicate-based access control (Wu et al. 2002) which largely helps in managing the workflow on an intra-organizational level. Further research has also been carried out which (Shen and Dewan 1992, Samarati et al. 2001) explores the management of the access control model on a multi user level. Overall it has also been concluded that these fundamental technical control mechanisms are believed to play an
important role in information security in a computer-based environment (Sandhu et al. 1995; Anderson 1972; Gordon & Loeb 2002).

**Proposition 1a:** Information security protection in supply chain can be achieved via technical implementation approach in each participant firm.

Besides, studies indicated that organizations should focus on formal and informal management to raise employee’s information security awareness (Thomson & Solms 1998; Webb et al. 2014; Safa & Von Solms 2016; Siponen 2001; Lin 2007; Mejias 2012; Tamjidyamcholo et al. 2014; Ifinedo 2012). The authors all agreed that most of the information security breaches are caused by human error, and employees as end-users are said to be “the weakest link” in information system security management in the workplace (Guo et al. 2011; Chen et al. 2006; Bulgurcu et al. 2010; Sindhuja & Kunnathur 2015). Similarly, several studies on supply chains pointed out that employees should consider information security as the top priority in order to protect not only themselves but also protect other employees and the whole organization from security breaches (Sindhuja 2014; Autry & Bobbitt 2008; Sindhuja & Kunnathur 2015).

Studies confirmed that formal management is significantly effective in cultures with high power distance (Robles et al. 2014). Indeed, high power distance societies tend to place a high valuation on the willingness of the top management, hence, are likely to open to top-down knowledge flows (Ford & Chan 2003). In an organisation with such a cultural background, if the top management believes in the importance of information protection and demonstrates efforts into raising awareness of its employees, it is highly likely that the organisation will successfully manage its information security (Ford & Chan 2003).

Researchers suggested that employees should be trained to reinforce their technical skills and information security knowledge. (Siponen 2000) emphasised that many information security techniques or procedures can be misused, misinterpreted or not used by end-users if they are not aware of potential threats. Training and empowering employees to handle unforeseen situations, hence, would be significant aids in the event of an exploited vulnerability or disruption (Autry & Bobbitt 2008). Besides, organizational impacts such as rewards and punishment are believed to influence employee’s behavioural intentions to compliant with information security policies (Feledi et al. 2013; Lin 2007; Ifinedo 2012). It is also the responsibility of organisations to ensure information security protection plans and policies are comprehensive so that employees can understand and be compliant with (Von Solms & Von Solms 2004; Shaw et al. 2009). The formal approaches become important considering a number of previous studies. (D’Arcy & Hovav 2007) highlighted security awareness programs among employees performing poorly as part of the security countermeasures in organizations. Their research emphasised the role education plays in the compliance of either preventive or monitoring technical controls in the workplace. In addition a recent literature review finds six critical success factors for successful security management which includes business alignment, organizational support, IT competencies, and organizational awareness of security risks and controls, information security controls and performance evaluation (Tu and Yuan 2014) which highlights again the importance of organizational awareness to the security implications of an organization.

**Proposition 1b:** Information security protection in supply chain can be achieved by formal approach in each participant firm.

To the informal management, on the other hand, scholars emphasised the importance of collaboration environments in workplaces where employees comfortably communicate and share their information security knowledge to each other in order to increase their awareness of potential risks and how to handle them (Tamjidyamcholo et al. 2014; Safa & Von Solms 2016; Smith et al. 2007). Sharing knowledge informally can be considered as the most efficient method used to encourage employees to participate in protecting information security that should be employed through social network communication. Studies suggest that organisations in developing countries may find it easier to develop an information sharing environment, compared to its counterparts in industrialised countries. According to (Ford & Chan 2003),
collectivistic cultures put priorities on collective accomplishments. Therefore, knowledge as a source of competencies and a tool to success, is considered to be shared to benefit the good of a group or a society.

**Proposition 1c:** Information security protection in supply chain can be achieved by informal implementation approach in each participant firm.

5. **Information Security Implementation at Inter-organizational Level**

In the modern time, organisations no longer manage their operations alone but rather form collaborations and partnerships with other firms to fulfil customers’ demands. The trend is also enhanced by developing countries when it comes to uncertainty avoidance. Indeed, uncertainty avoiding organisations always seek predictability and an establishment of regulations and integrated operations. In the supply chain context, they would reinforce information sharing and collaboration with their partners to maximise the use of stocks and transportation in order to obtain certainty (Cao & Zhang 2013).

Nevertheless, inter-organizational information sharing is posing severe threats and financial losses to organisations. Supply chains have been heavily relying on the technical infrastructure for data exchange. Information is growing at an enormous rate while supply chain partners are sharing intellectual assets through a number of internet based mechanisms (Humphreys 1994) that are open to a wide array of security breaches (Kunnathur 2015). Therefore, it has become vital for every organisation to be protected and to protect their information assets in a collaborative environment (Li, Du & Wong 2007).

The need for higher information security leads to that for a higher level of trust among the supply chain partners, which can be achieved through designing a secure and robust access control mechanism. Indeed, technical security mechanisms allow the supply chain partners to exchange and share information seamlessly (Li, Du & Wong 2007) as well as sustain profits of the whole supply chain performance (Li & Zhang 2008).

Nevertheless, to design and develop an effective information network within a supply chain is a great challenge for any of its parties. Many supply chains protect their information flows by selecting one of their parties as an information hub to collect information from customers, process, and share it with suppliers to the upstream (Zeng et al. 2012). However, Zeng et al. (2012) discussed that manufacturing firms being focal in the networks are likely to be in conflicts and unintentionally create legal issues. To tackle this issue, researchers and practitioners introduced the use of Radio Frequency Identification (RFID) in order to encourage participants to share process data to achieve the target of collaboration and ensure the integration flow (Chow et al. 2007). Although the model improves the real-time information sharing among supply chain members through integrating web-based and auto-identification technologies, it may bring about new privacy and security issues to the collaboration networks (Michael & McCathie 2005).

Zeng et al. (2012), then reviewed the different infrastructure and technology controls among networks and concluded that there are four collaboration solutions practitioners should implement for better secured information sharing. i.e. computer security and privacy technologies, access control, secure multiparty computation, and location-based service (Zeng et al. 2012). Firstly, there has been a number of scholars highlighted the importance of computer security and privacy technologies. (Pereira 2009; M. Voss et al. 2009; Chow et al. 2007; Sindhuja & Kunnathur 2015) implied that each member of a network should consider compatible technical security controls at both ends to secure the flow of information. The technical controls should focus on the authentication and access control mechanisms for inter-organizational communication and exchange of information, and also set up network security controls and cryptographic techniques for uninterrupted and secured flow of information along the supply chain (Sindhuja & Kunnathur 2015). Secondly, collaborative access control provides...
a shared secure environment that allows partners to be authenticated via multiple networks that are mapped to the each network player’s data (Jonscher & Dittrich 1994; Zeng et al. 2012). Thirdly, Secure Multiparty Computation (SMC) is a shared mechanism of joint secure working in inter-organizational networks (Zeng et al. 2012). SMC method can be used to control the secure transmission of information and its synchronisation without any information trickle by concealing cryptographic algorithms (Atallah et al. 2003). Finally, Location-Based Services (LBS) is an excellent technology that can identify and calculate user locations and movements without disclosing their personal identifiable information. This feature is consequently very helpful for covering real locations of various users within a system with wrong location data that in turn, ensures a risk-free information sharing environment (Zeng et al. 2012). Besides, manufacturers can use LBS for not only following humans who carry electronic devices such as mobiles and laptops but also tracking consumer behaviours and good distributions. For instance, they can add sensor identifiers, which are often low-cost, to products and be updated whenever the products are processed through stages of the supply chain (Jiang & Yao 2006). By deploying these shared controls at supply chain levels, information shared among the supply chain partners can build a trust culture and positively impact on the strategic relationships.

**Proposition 2a:** Information security protection in supply chains can be achieved by collaborating in technical security controls.

Scholars implied that all parties within a supply chain need to collaboratively create and commit to a comprehensive information security plan to avoid any information security risks from external attacks (Smith et al. 2007; M. Voss et al. 2009). In fact, (M. Voss et al. 2009) found in their study on the food industry that firms tend to focused on internal operations and do not recognise the importance of collaborating in protecting their information flows until they experienced security problems. Furthermore, there are many organisations aware of information security risks within their supply chains but not actively disseminate information security policies with their partners (D. M. Voss et al. 2009). A supply chains in which firms spend the least concern on collaboration in protecting information security can foresee its disruptions and vulnerabilities (Smith et al. 2007).

Many research suggest supply chain parties to collaborate in planning, forecasting, and replenishment to ensure their information flows are always accurate, available, and in real-time. According to (Knight 2003), security planning, aforementioned controls, and procedures should also be formalised by adding them to contract documents, which also commits the trading partners to agreements of consequences and sharing of hazardous situations. Each party, then, has to proactively implement the shared policies at all of its levels by raising awareness among its staff members through training and management (Knight 2003). Besides, (Woolthuis, Hillebrand & Nooteboom 2005) recommend that sharing best information protection practices among supply chain partners can contribute to a higher awareness of security practices while building up mutual trusts within their networks (Woolthuis, Hillebrand & Nooteboom 2005).

**Proposition 2b:** Information security protection in supply chain can be achieved by collaborating in planning and committing in information security issues.

Sharing information security knowledge, nevertheless, should go beyond the supply chain network boundaries since it is an effective way to deter attacks from outside hackers, thereby indirectly increase the effectiveness of security technologies (Schechter & Smith 2003). Several studies suggested that firms should join in coalitions supported by governments where they can share and learn about each other’s information security problems (Gal-Or & Chose 2005; Phillips et al. 2002; Schechter & Smith 2003). The practice contributes to raising firms’ awareness of potential risks that might occur in their operations so that better preventing, correcting and detecting of further security breaches in the future could be achieved (Gal-Or & Chose 2005). In addition, (Sindhuja & Kunnathur 2015) suggested that this is a great opportunity for employees of participative organisations to informally communicate as a way of a social networking via elevator conversations, phone calls, etc. As such, firms within a
supply chain should collaborate and nurture a cultural climate that is conducive for supply chain information security system, and that they should interact with each other to ensure a certain amount of controls at the informal security level (Sindhuja & Kunnathur 2015). Zhao & White (2012) provided a collaborative information-sharing model that ensures cyber security in the supply chain community. They argued that effective information sharing regarding inclusive security incidents would encourage supply chain partners to collaboratively handle problems (Zhao & White 2012). Iyer, Fergle & Singh (2008) introduced and enhanced the use of CPFR model in supply chains in order to improve information security practices. Persadha et al. (2016) proposed a security information sharing model for effective collaboration among members within supply chains that in turn, contributes to improving Indonesia's national security. The researchers concluded that education, trust, reward systems, leadership communication, and IT platforms are key elements to enhance knowledge sharing that in turn, will improve security awareness.

**Proposition 2c:** Information security protection in supply chain can be achieved by sharing information security knowledge formally and informally.

### 6. Conclusion and Directions for Future Research

Information security has been increasingly a popular topic in supply chain management due to the development of modern technology. The main target of this paper is to address the gap in literature and in practices in regards to information security in supply chain management. Indeed, there have been inadequate perspectives focusing on technologies to ensure information protection. Human aspect in information management, including formal and informal, is more complicated to develop and implement but extremely essential since it addresses the most vulnerable components of the system. Evidences from literature undoubtedly suggest that an awareness of information protection need to be spread widely to all employees of supply chains partners and that there should be considerable incentives that reward those with strong understandings of the issue. Gaining controls at all aspect of information management could be a step towards stronger supply chain partnerships.

The paper also addresses the lack of cultural implications of previous research by considering the topic with special attention to particular cultural dimensions of the developing country context. As we found the connection between cultures and information management practices, it is to suggest that both professionals should pay more attentions when planning and implementing strategies and processes. While technical controls are insignificantly altered by cultural features; human perspectives should be a key factor to define formal and informal management practices. Indeed, professionals may find it is impossible to replicate best practices from one country to another. Due to cultural and conditional disparities, one practice may not work the way it does in other contexts. This paper also suggests future scholars to examine the idea yet explore further to leverage cultural factors on better supply chain management.

From a technical perspective, the paper has reviewed a number of technologies and suggests that some of them possibly cause side effects to information security systems although they bring about greater opportunities of knowledge generation and sharing. That is, the authors propose that future research on the technical aspects of information security gain further experience and understandings of different tools, that is, find and develop the best technologies to implement in supply chains.

**References**


IJISE is a FTMS Publishing Journal