Chapter 13
Trust-Based Information Risk Management in a Supply Chain Network

Yanjun Zuo
University of North Dakota, USA

Wen-Chen Hu
University of North Dakota, USA

ABSTRACT

Information risk management is crucial for an organization operating in an increasingly integrated and intensively communicated environment to mitigate risks and ensure core business functions. Given the open and dynamic nature of a supply chain network, information risk management is challenging and various factors must be considered. This article introduces a trust-based approach to facilitate supply chain participants to perform effective risk management. The major components of the proposed framework include supply chain member trust evaluation, data classification, and trust-based decision making. The major purpose of the framework is to control and mitigate information risks that a participant faces in a supply chain network (e.g., risks to information confidentiality, privacy, and integrity). We apply the principle of transitive trust for trust evaluation and use several decision tools for risk analysis and mitigation.

INTRODUCTION

A supply chain connects material suppliers, manufactures, whole sellers, regional distributors, and retailers to closely collaborate to achieve more operational efficiencies. It covers all the entities and activities involved in movement and storage of raw materials, work-in-process inventory, and finished goods from point-of-origin to point-of-consumption. Strictly, a supply chain is a network (Kroenke, 2008). Chains imply that each organization is connected to just one company up (towards the supplier) and down (towards the customer) the supply chain. This is not a case. At each level, an organization can work with many organizations both up and down the supply chain. So, various channels exist from a supplier to a customer. Essentially, those channels create a network (Kroenke, 2008).

DOI: 10.4018/978-1-60960-135-5.ch013

Close cooperation among supply chain partners creates needs for effective communications. Information technologies have made information sharing and data exchange convenient (Yu, Yan, & Cheng, 2001; Andersen, 2001; Bradley, 1999). But new technologies also bring new challenges. When business becomes more global, more information simply needs to be shared. When more information is needed to be shared, more security problems could happen. When systems become complex to deal with those problems, more things simply could go wrong. Particularly, when system interdependencies become a norm, cascading effects can take place and cause threats to data and systems: a compromised system could continue to compromise another system, referred as secondary or subsequent attack (Yue, Cakanyidirm, Ryu, & Liu, 2007; Ammann, Jajodia, & Liu, 2002). Supply chain participants must carefully study the threats in an information technology intensive environment and take effective methods to mitigate risks that could interrupt their crucial business operations.

A full cycle of risk management includes risk identification, risk analysis and risk mitigation. Effective risk management is to (1) identify any potential risks that an organization faces (including cyber attacks from external malicious hackers, internal human errors, and system failures); (2) assess the levels of threats to the organization's assets, and (3) develop strategies and approaches to mitigating risks. Before any security mechanisms are deployed, it is essential that an organization first poses a clear understanding of their security risks, conduct solid risk analysis and develop effective risk mitigation policies.

This article introduces a trust-based risk management framework to address information security in a supply chain network. Trust is a fundamental concept in many social and commercial activities and has been studied in various disciplines. Mutual trust among participants is a prerequisite for the success of a supply chain network. Supply chain participants collaborate based on established trust relationships among member with mutual benefits and common objectives. Many factors affect the trust of one entity for another: (1) cognition (observation)-based, e.g., privacy protection, security protection, (2) affect-based, e.g., reputation, presence of third-party seals, referral, (3) experience-based, e.g., familiarity, Internet experience, and (4) personality-oriented, e.g., disposition to trust (Kim, Ferrin, & Rao, 2008). Trust and risk are closely related. Risk is defined as potential threats or damage that may cause to a given system. More specifically, supply chain risk refers to an uncertainty or unpredictable event affecting one or more of the parties within the supply chain or its business setting which can (negatively) influence the achievements of a business's objectives. Although there are different views about their relationship, many scholars agree that trust can effectively reduce risk. According to Chopra, & Wallace, 2003, trust is defined in terms of willingness to assume risk, intention to make oneself vulnerable, acceptance or risk, and readiness to assume risk. When the complexity and scope of a virtual community like a supply chain grows large, trust becomes a necessary mean for a participant to deal with any uncertain and uncontrollable activities of other members in the community. Trust alleviates the risks in a supply chain network. Individual participant can rely on trust to minimize the uncertainty of future events by predicting their results based on past experiences (represented as trust relationship between a trustor and a trustee).

Many information risks in a supply chain network can be tracked back to communications and information sharing among supply chain partners. Suppliers, intermediaries, third-party service providers, and manufacturers use integrated systems to process and share information in order to quickly seize market opportunities and achieve competitive advantages. Members often need information from their partners in order to make correct decisions. For instance, a material supplier needs production plan data of