Chapter 101
Information Security Compliance Behaviour of Supply Chain Stakeholders:
Influences and Differences

Ibrahim Shafiu
Auckland University of Technology, New Zealand

William Yu Chung Wang
Auckland University of Technology, New Zealand

Harminder Singh
Auckland University of Technology, New Zealand

ABSTRACT

Supply chain security is an emerging topic in the supply chain management literature. Information security is a key component of supply chain security, and this study aims to identify the factors that influence the compliance behaviour with respect to information security. A related objective is to understand the extent to which compliance was substantive or symbolic. Adopting a qualitative approach, the authors conducted semi-structured interviews with stakeholders based in New Zealand who are involved in international supply chains. The interviews find that compliance behaviour is affected by the influence of other organizations, organizational perceptions of compliance, and the rules and norms of exchange in different contexts. The results also indicate that compliance behaviour is more symbolic than substantive in the supply chain environment.

DOI: 10.4018/978-1-7998-0945-6.ch101

INTRODUCTION

Supply chain security (SCS) is an emerging field of research within the supply chain management (SCM) discipline. Security is a key concern for SCM because supply chains are complex, vulnerable and fragile because they are made up of interdependent stakeholders who rely on their partners' trustworthiness and commitment (Sarathy, 2006). With the need to protect national borders against terrorists using conveyances or containers to ship weapons of mass destruction or harmful bio-weapons, SCS has become an even more important issue for many countries (Closs & McGarrell, 2004; Lee & Whang, 2005; Urciuoli, 2010). However, little empirical literature supports policy or practice in this emerging field (Williams, Jason, & Stephen, 2008).

Closs and McGarrell (2004) define supply chain security as: "the application of policies, procedures, and technology to protect supply again assets (products, facilities, equipment, information and personnel) from theft, damage, or terrorism, and to prevent the introduction of unauthorised contraband, people or weapons of mass destruction into the supply chain" (page 8).

SCS comprises elements such as information sharing (Closs & McGarrell, 2004), information security (Lee & Wolfe, 2003), and information gathering for intelligence (Flynn, 2000). Information security is a key component of ensuring security in supply chain operations, especially in multi-tier supply chains where a single security breach could expose all partners to the risk of a leak of valuable information (Tang & Zimmerman, 2013). This information may include sensitive governmental information which could have ramifications for national security if criminal organizations obtain it (Bhargava, Ranchal, & Ben Othmane, 2013).

Government authorities working within global supply chains obtain information from traders and related stakeholders through the enforcement of various supply chain security initiatives. These security initiatives have now become global schemes, as firms, along with their international supply chain partners and the corresponding governments, have to collaboratively monitor and safeguard security at all points of the cross-border cargo movement process (Sarathy, 2006). Examples of these global supply chain security initiatives include the Container Security Initiative (CSI), the Advanced Manifest Rule, and the Customs-Trader Partnership Against Terrorism (C-TPAT) developed by the United States of America and the International Ship and Port Facility Security (ISPS) code developed by the International Maritime Organization (Sarathy, 2006). For instance, the Advance Manifest Rule requires exporters to the United States to forward their manifest information 24 hours before their vessel departs for the United States. But, if they do not provide the appropriate level of information security, the rule's objective of securing the supply chain is not achieved.

The criticality of SCS indicates a need to examine security-related behaviours at the organizational level. However, there is little research in the information security field on the organizational and social aspects of security-related practices, with the dominant topic of research being data management (Dhillon & Backhouse, 2000). In addition, there are only a few studies on information security in information management journals, and the number of theoretical papers in information security research is also low (Dhillon & Backhouse, 2001; Smith, Winchester, Bunker, & Jamieson, 2010). Information security research is particularly under-represented in the leading information systems journals (Bulgurcu, Cavusoglu, & Benbasat, 2010), as well as operations and management journals. This may be due to the intrusive nature of such research, necessitating a significant level of trust between the organization and the researcher (Smith, et al., 2010).