The impact of supply chain security practices on security operational performance among logistics service providers in an emerging economy

Security culture as moderator

Suhaiza Hanim Zailani
Faculty Business and Accountancy, Universiti Malaya, Kuala Lumpur, Malaysia
Karthigesu Seva Subaramaniam
Graduate School of Business, Universiti Sains Malaysia, Penang, Malaysia
Mohammad Iranmanesh
Faculty of Business and Accountancy, University of Malaya, Kuala Lumpur, Malaysia, and
Mohd Rizaimy Shaharudin
Faculty of Business Management, Universiti Teknologi MARA, Kedah, Malaysia

Abstract
Purpose – The security issue in supply chains is among the most pressing concerns that firms are currently facing. As a preliminary attempt to address this lack of empirical research, the primary purpose of this paper is to explore the relationship between security practices and the security operational performance with respect to security culture as a moderator.

Design/methodology/approach – With the resource-based view of the firm as the theoretical underpinning, the study utilizes survey data to test the propositions derived from the security literature and partial least squares for the analysis.

Findings – The research reveals four crucial practices of supply chain security that collectively affect a firm’s security operational performance among Malaysian service providers. It is also interesting to observe that security culture positively moderates the relationship between facility management and the security operational performance of the firm.

Research limitations/implications – Firms in emerging countries need to realize that supply chain security practices can result in significant benefits to their firms that can give them additional incentives to adopt these initiatives. This study may also help policymakers in emerging countries, in general, in setting appropriate policies and strategies, and Malaysia, in particular, for ensuring that it is a secure location for exporting cargo and giving assurance to the local and international investors to continue their investment.

Practical implications – This study will assist supply chain managers and logisticians to re-examine their existing supply chain security model by considering the selected supply chain security practices, which have a significant impact on supply chain security operational performance. Individual firms need to strategize their business model with the inclusion of security aspects, which will surely create a competitive advantage over other players in the logistics industry. Firms can develop the best appropriate supply chain security model that will benefit the firm, customers, and business partners, such as suppliers and local authorities.
The impact of supply chain security practices
Supply chain management (Sheffi, 2002, 2005a, b; Rice and Caniato, 2003; Christopher and Peck, 2004; Peleg-Gillai et al., 2006).

Most of the literature on supply chain security practices has been written from the perspective and experience of developed countries (USA, Europe, and Japan), and few studies have studied supply chain security practices in the context of emerging countries like Malaysia. With the exception of the study of Yang and Wei (2013), no other study has been found that empirically investigates the effect of supply chain security on security performance in the South East Asian region generally. That is, the proposed or suggested practices for managing supply chain security have not been validated in emerging countries. Furthermore, despite its importance, little or no research exists concerning how security culture in countries, such as Malaysia, may affect the relationship between supply chain security practices and security performance. As a result, little is known about how security culture influences the scope and deployment of supply chain security activities and thereby differentiates firm security performance. It is important to bear in mind that the organizational culture for companies in Asia (including Malaysia) is totally different from companies in other countries (Cullen et al., 2004; Morris et al., 1998). Because of the continuing increase in global competition, regardless of whether manufacturing firms act proactively or reactively, an investigation of the role of security culture offers substantial value to practitioners. In addition, an investigation of the role of security culture may refine our conceptual understanding of the linkages between supply chain security practices and performance, especially in the context of developing countries.

To summarize, in an attempt to partially address the lack of empirical research, this study aims to investigate the effect of supply chain security practices on security operational performance by considering security culture as a moderator. This study hopes to provide primary guidelines for government agencies that are developing policies and strategies to ensure Malaysia is a secure location for exporting cargo and give assurance to the local and international investors to continue their investment. This study contributes to the literature using a theoretical foundation from the resource-based view (RBV) of the firm to test empirically the propositions developed from past studies on supply chain security. The scope of this study focuses on the human and organization capital aspects of RBV and the perceptions of managers concerning the security operational performance of firms. The following sections discuss the theoretical foundation and supply chain security literature from which the research propositions are derived. Next, the survey research methodology for data collection and the econometric model used to test the propositions are discussed. Finally, the research findings and study implications are presented.

**Literature review**

**Supply chain security practices**

The supply chain management literature provides little help in understanding supply chain security (Closs and McGarrell, 2004; Hale and Moberg, 2005; Williams et al., 2008) and there is a gap in academic research to address security-related issues in supply chain management. Although a few authors, such as Sheffi (2001), Gutierrez et al. (2007), Sheu et al. (2006), Closs et al. (2008), and Hintsa et al. (2009), have discussed the importance of security initiatives in the supply chain, these initiatives have only been discussed conceptually and have not been tested empirically. Van Oosterhout et al. (2007) presented a case study about the Port of Rotterdam on visibility platforms.
for enhancing supply chain security, in which they mentioned that a secured supply chain refers to a supply chain in which various measures have been taken to guarantee a certain level of security while operating.

Van Oosterhout et al. (2007) commented that there are two main categories for supply chain security measures. The two categories are preventive measures and corrective measures. The preventive measures consist of physical security and nonphysical security, such as facilities security, cargo security, information security, and human resource management security, the preventive measures focus on preventing the occurrence of security-related risks in the supply chain, while corrective measures focus on limiting the impact caused by security-related risks. Hence, another way for supply chain owners to protect their supply chain would be by undertaking proper corrective action when an unpredicted crisis occurs in the supply chain. Whenever a supply chain faces a crisis, corrective action will help firms to return to a normal state quickly. Resilience management and business network management is an example of the corrective measures approach (Sheffi, 2005a; Van Oosterhout et al., 2007).

Security culture
The development of a formal or informal culture in organization can convey the norms and behaviour, form of communication design, information practise and distribution, anticipated performance and outcomes and customs (Anderson and Ackerman, 2001). As such, the organizational culture imposes the expectation over the employee’s performance (McAfee et al., 2002) and can be leveraged by managers as a strong tool for them to manage the employees to meet the organization’s objectives (Tichy, 1982).

In the most general sense, the term security culture refers to the employee’s awareness, combined with the real things that are done (Frederick, 1995). Thus, the involvement of humans in security is highly essential; including their participation in the development of policies and business design that will lead to an appropriate security culture in the organization (Ekwall and Rolandsson, 2012). The spread of security culture among employees can assist the management in designing appropriate security policies through the interaction and involvement of employees in order to minimize the overall risk attributed by security problems. According to Ekwall and Rolandsson (2012), most company security programmes stress on the need for high awareness among employees in pursuance of enhancing the overall security level. Good awareness pertaining to the issue of cargo theft must be a part of the implicit rules governing the employees conduct or in different terms, can be known as the security culture without the direct written procedure or regulation. However, security culture is contingent on the complexity of each company and it is imperative to have employees that can manage security issues independently in global and complex organizations (Ekwall and Rolandsson, 2012).

Supply chain security operational performance
Security performance can generally be assessed by hard (objective) measures and soft (perceptual or responsive) measures (Dalton et al., 1980; Shang and Lu, 2009). Because actual incident data are difficult to obtain and perceptual measures are valid indicators of security performance (Shang and Lu, 2009; Voss et al., 2009), this study used perceptual-based measures to assess the security performance of logistics services providers. Security performance is defined as the measurement and comparison of actual levels of achievement with regard to security. It is related to the prevention of any malicious threat, damage, and disturbance to an organization. Many studies...
have identified performance indicators of security performance. Although the implementation of security initiatives can result in additional cost, supply chain security management has several benefits, including a reduction in theft, cybercrime, terrorism, smuggling, counterfeit goods, and damage to goods (Gutierrez and Hintsa, 2006; Martens et al., 2011).

According to a report published by the European Commission (2007), enhancing supply chain security can reduce theft and losses, reduce the number of delayed shipments, improve planning, increase customer loyalty and employee commitment, reduce the number of safety incidents, lower inspection costs of suppliers and increase cooperation with them, reduce crime and vandalism, and improve security and communication between supply chain partners. Furthermore, security management facilitates international trade by reducing transit time (Banomyong, 2005), improving customs clearance efficiency (Sheu et al., 2006; Peleg-Gillai et al., 2006; Diop et al., 2007), and increasing port operational efficiency (Bichou, 2011; Yang, 2011). It also helps businesses predict the movement of goods and lead-time, decrease the number of customs inspections, reduce the time taken to release cargo by customs and waiting times at borders, and increase supply chain visibility (Diop et al., 2007). To summarize, an efficient and secure supply chain can lead to higher visibility and an increase in supply chain efficiency and customer satisfaction, reduction in lead-time and overall cost reduction. This study used a composite measure of performance covering these dimensions to evaluate the supply chain security operational performance, which is considered as preventing the security performance of logistics service providers in Malaysia.

In conjunction with this, the second-order construct is used to model a level of abstraction higher than those from first-order constructs alone. The model also captures the multidimensional nature of security performance which security performance well because each dimension represents some portion or aspect of the overall latent construct (security performance). Using a multidimensional construct provides the ability to increase granularity and detail on different aspects of a construct (Petter et al., 2007).

**Theoretical background**

Although SCM scholars have dedicated considerable effort to understand the relationship between supply chain security and security performance (Voss et al., 2009; Yang, 2011; Yang and Wei, 2013) the existing literature offers conflicting empirical findings about the performance implications of supply chain security. Overall, the mixed results pertaining to this link suggest the need for a contingency perspective to explain the relationship. Two important questions must be addressed to resolve this inconclusiveness. First, practitioners need to know whether the supply chain security practice, as a firm-specific resource, is itself a source to enhance security performance. Second, existing research examining the supply chain security practices-performance linkage has overlooked potential moderating variables. To answer the first question, we test the supply chain security practices-security performance relationship in our model by considering supply chain security practices as an antecedent mechanism that aids in the translation of security resources into performance. More specifically, we posit that a supply chain wide emphasis on security has a positive impact on firm security performance. In response to the second query, this study investigates security culture as a moderator in supply chain security practices-security performance research to help derive guidelines for firms seeking to improve their performance through supply chain security.
This research is explicitly grounded on the theoretical foundation of the RBV. The RBV theory is useful to investigate the relationship between the internal organizational capabilities and the service provider’s performance (Barney et al., 2001). In the RBV theory, resources are all the tangible and intangible assets that firms use to conceive and implement their strategies (Wernerfelt, 1984; Rumelt, 1984; Barney et al., 2001). The RBV theory has three important constructs – resources, capability, and competencies (Yang et al., 2009). The RBV of the firms suggests that combining resources, including cargo, facilities, information, and humans can generate unique and hard-to-imitate capabilities that contribute to supply chain security performance. The firms that can manage their resources and capabilities in a supply chain more efficiently are likely to gain competitive performance (Dangayach and Deshmukh, 2001). The supply chain security practices are the capabilities which are distributed heterogeneously across firms and cannot be transferred from a firm to another without cost. Therefore, successful supply chain security requires adaptation of the RBV because the resources and capabilities are two valuable factors for supply chain security (Martens et al., 2011).

Security measures will help to protect firms from any unexpected supply chain incidents and work as a detection system for supply chain players in the case of any disaster. Typically, companies pursue security initiatives to protect their supply chain. Hintsa et al. (2009) grouped security measures into four categories, namely, cargo management, facility management, human resource management, and information management, which are used in the current study as independent variables. The independent variables of the current study (Figure 1) are mainly related to resources and are fully supported by the RBV theory. The cargo and facilities are the physical and tangible assets of a service provider in the logistics industry (Javidan, 1998; Carmeli, 2004; Kaleka, 2002; Hafeez et al., 2002) while place constitutes the resource part of the RBV theory. Information is a firm’s source of competence (Yang et al., 2009; Hafeez et al., 2002) and human resource is a source of knowledge, which falls in the capability part of the RBV theory.

### Conceptual framework and hypotheses development

Sarathy (2006) posited that security measures impose high cost on firms during implementation, but that they give long-term benefit for firms by improving the overall performance of the supply chain. Bearing Point (2003), a consultation firm, undertook a study of the financial impact between shippers and customers from Thailand and the USA by implementing a secure supply chain management system. The report studied the benefits to the service providers, for which the results show that there is a

![Figure 1. Proposed theoretical model](image-url)
relationship between security initiatives and financial performance. The security efforts led to certain financial benefits: better visibility on cargo arrival timeline and cargo monitoring; avoidance of cost on US customs' trade security measures; reduction in size of inventory; increase in sales; and reduction in theft and pilferage. Peleg-Gillai et al. (2006) also studied the security measures that lead to organizational performance if security implementation is undertaken in a proactive rather than reactive manner.

To guide the development of our conceptual framework, we depict the key constructs in Figure 1. On the basis of our literature review, we propose that supply chain security practices and security culture play different roles in contributing to firm security operational performance. We propose that supply chain security practices encompassing cargo management, facility management, human resource management, and information management relate to firm security operational performance, such as higher visibility increase in supply chain efficiency and customer satisfaction, reduction in lead-time and overall cost reduction. We further propose, that security culture influences the relationship between supply chain security and security operational performance. The following sections provide a brief review of the literature pertaining to each practice. In addition, research propositions suggested by the literature are offered.

**Cargo management and security operational performance**

Cargo management refers to protecting the cargo during all the steps of the manufacturing, shipping, and transport processes (Hintsa et al., 2009). Organizations implement security measures to protect the supply chain against potential risk (Closs et al., 2008). Cargo is one of the major sources of security concerns in the supply chain (Sarathy, 2006). The common security issues while handling cargo are theft, which causes a great disturbance in the supply chain (Chapman et al., 2002; Ekwall, 2009). The trend for cargo theft in Asia is increasing rapidly, and Malaysia and the Philippines have the highest cargo theft cases among all the countries in Asia (FreightWatch International, 2011). In order to protect cargo throughout the logistic activities, cargo management is needed as a security practice by the service provider in the logistics industry (Gutierrez and Hintsa, 2006). Cargo-related incidents could impact firm performance and cause tangible and intangible damage to an organization (Securitex, 2008). Bearing Point (2003) stated that among the security efforts firms can obtain through physical security initiatives are better visibility of the cargo arrival timeline and cargo monitoring. Since security is a new topic, firms may have a lack of exposure to understand how security initiatives will have a positive effect on security performance (Voss et al., 2009). Hence, the following hypothesis is formed:

\[ H1. \text{Cargo management positively affects supply chain security operational performance.} \]

**Facility management and security operational performance**

Facility management refers to the integrated management of the workspace to enhance the performance of the organization (Tay and Ooi, 2001) by guaranteeing the security of the facilities where the cargo is stored and handled (Hintsa et al., 2009). Optimal warehouse/terminal layout designing (e.g. entry/exit controllability; clearly marked control areas; sufficient lighting conditions) and efficient facility monitoring (e.g. 24-hour camera system, security guards, filming activities of loading containers, and picking) are the most common facility management practices (Hintsa et al., 2009). Protection of the facility is needed as many valuable resources, products, cargo and
important information are stored in a firm’s facility and any security-related disaster may affect the performance and operating environment of the firm. Hence, the following hypothesis is drawn:

\[ H2. \text{ Facility management positively affects supply chain security operational performance.} \]

**Human resource management and security operational performance**

Employee screening and hiring practices are one of the important aspects in supply chain security (Rice and Caniato, 2003). Employees with low loyalty to the firm may undertake intentional acts of sabotage and impair the performance of the firm (Lensing, 2003). By practicing proper screening and hiring (e.g. background checks; interviews for leaving, or employees who have been fired), firms can prevent hiring employees who have the potential for being an enemy to their own supply chain (Hintsa et al., 2009). Human resource management guarantees trustworthiness and security awareness of all personnel in direct and indirect contact with cargo and other company assets (Hintsa et al., 2009). Therefore, the current study hypothesizes that:

\[ H3. \text{ Human resource management positively affects supply chain security operational performance.} \]

**Information management and security operational performance**

Information serves as the basis for decision making and generates value for organizations. Improper management of information may lead to irreparable damage to organizations (Michelberger and Labodi, 2009). Information pertaining to a firm’s business activities and transactions are usually shared with supply chain partners and protecting this information from outside intruders or competitors is critical for the success of firms in the competitive market (Kolluru and Meredith, 2001). Hence, service providers in the logistics industry must have proper security measures to protect the information. Hintsa et al. (2009) defined information management from the supply chain security management perspective as protecting critical business data and exploiting information as a tool for detecting illegal activities and preventing security breaches. Having complete information about supply chain activities, both downstream and upstream, also helps to avoid security breaches and protects all the other members in the supply chain. Thus, we set the following hypothesis:

\[ H4. \text{ Information management positively affects supply chain security operational performance.} \]

**Moderating effect of security culture**

Supply chain researchers rely on the importance of understanding organizational culture. Tan et al. (1998) suggested that organizational culture is one of the most critical elements for supply chain members to grasp as they seek to optimize the performance of their overall system and their individual firm acting within it. On the other hand, according to Williams et al. (2009), the implementation of security is the culture of the organization in respect of the way that security interacts with the organization’s employees in terms of sustainable norms and expectations.

Although supply chain security research is still in its infancy stage, researchers in the area of security of supply chains have begun to incorporate the effects of organizational culture (Closs and McGarrell, 2004; Hale and Moberg, 2005; Williams et al., 2009). Sheffi (2005a) claimed that the most important element of security in the supply chain is culture: the building of a security culture is a cooperative initiative
between the employees and management. In conjunction with this, Autry and Bobbitt (2008) investigated the behaviour of employees towards security practices as they performed their daily tasks and found that firms with security-oriented employees may enjoy several organizational performance advantages. This supports the argument of other researchers that supply chain security practices are related to the importance of human attitude, HR practices, and other employee-level effects on organizational performance (Christopher and Peck, 2004; Closs et al., 2008; Rice and Spayd, 2005; Sheffi, 2002, 2005b). By establishing a security culture among the workers at the base level through the delegation of authority, the protection of supply chains will be at its highest level and able to handle and solve any security issue in the supply chain (Autry and Bobbitt, 2008). It suggests that, security culture creates an opportunity for firms to safeguard their supply chain operations and will help firms to implement security initiatives more effectively, thus it is expected that the existence of a higher security culture enhances the positive effect of security initiatives practices on supply chain security operational performance. Hence, the following hypotheses are developed:

\[ H5. \text{ Security culture moderates positively the effects of (a) cargo management, (b) facility management, (c) human resource management, and (d) information management on supply chain security operational performance.} \]

**Research methodology**

**Sample and data collection**

The unit of analysis for this study is service provider firms in the logistics industry that operate in Malaysia. In Malaysia, the service providers in the logistics industry are divided into two categories – transport service provider and service provider. In this study, the unit analysis will cover both types of service provider in the logistics industry. Questionnaires were mailed to 800 target respondents who hold executive positions or higher in the service provider firms. The firms were selected from the Malaysia logistics directory 2011/2012. Out of 226 responses received, five of the responses were partially completed, 15 were discarded in data cleaning, resulting in an effective response rate of 25.75 per cent (206/800). Considering the length of the survey, this response rate is quite satisfactory and compares favourably with other empirical studies in supply chain management (Stanley and Wisner, 2001; Chen et al., 2004). The final sample consisted of 20 (9.7 per cent) owners/CEOs/directors, 138 (67.0 per cent) senior managers/managers, and 48 (23.3 per cent) executives. The distribution mainly focused on freight forwarders (31.9 per cent), third-party logistics companies (20.9 per cent), container shipping companies (14.5 per cent), and container shipping agencies (10.9 per cent). In terms of the number of employees in the firm, the data indicated that 57.3 per cent of the firms have less than 50 employees.

**Measures of constructs**

This study employed a quantitative survey with a structured questionnaire. To develop measurement items, processes recommended by several authors in the literature was followed (Bienstock et al., 1997; Churchill, 1979; Gerbing and Anderson, 1988): item generation through literature review; academic expert review; debriefing with industry experts; and item purification in the empirical study.

First, we adapt measurement items relevant to the construct, based on prior literature. Table I summarizes the measurement items for each of the practices of supply chain
<table>
<thead>
<tr>
<th>Constructs</th>
<th>Items</th>
<th>Factor loadings</th>
<th>CR</th>
<th>AVE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cargo management (CM)</td>
<td>We have […]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Regular inspection during movement of cargo</td>
<td>0.849</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Adequate detection of shipping process anomalies</td>
<td>0.856</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Adequate supervision to avoid deviations in vehicles travel time</td>
<td>0.816</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Restricted access to documents related to cargo</td>
<td>0.781</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Appropriate identification for cargo</td>
<td>0.890</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Alternate plans for movement of cargo during emergency</td>
<td>0.839</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Facility management (FM)</td>
<td>Fire protection system</td>
<td>0.889</td>
<td>0.962</td>
<td>0.720</td>
</tr>
<tr>
<td></td>
<td>Sufficient lighting conditions</td>
<td>0.843</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Security guard to respond during emergency situation</td>
<td>0.861</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Clear identification of restricted areas</td>
<td>0.856</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Periodic inspection to assure integrity of security measures</td>
<td>0.863</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Restricted access to facility to only authorized personnel</td>
<td>0.894</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Camera-based systems that allow monitoring</td>
<td>0.865</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Monitor entry activities at facilities to avoid intrusion of unauthorized individuals</td>
<td>0.781</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Monitor exit activities at facilities to avoid intrusion of unauthorized individuals</td>
<td>0.815</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Physical obstacles to discourage theft in entering</td>
<td>0.811</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Human resource management (HRM)</td>
<td>Rigorous screening process before hiring our employees</td>
<td>0.778</td>
<td>0.882</td>
<td>0.714</td>
</tr>
<tr>
<td></td>
<td>Security training programmes for every employee</td>
<td>0.876</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Employee identification procedures</td>
<td>0.876</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information management (IM)</td>
<td>Processes to backup computer system data</td>
<td>0.773</td>
<td>0.866</td>
<td>0.684</td>
</tr>
<tr>
<td></td>
<td>Recordkeeping of information for potential security audits</td>
<td>0.903</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Data exchange between supply chain partners</td>
<td>0.800</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security culture (SC)</td>
<td>Senior manager views supply chain security as a competitive advantage</td>
<td>0.928</td>
<td>0.947</td>
<td>0.856</td>
</tr>
<tr>
<td></td>
<td>Make sure that supply chain security is the first thing on the mind of all employees</td>
<td>0.922</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Make supply chain security the norm for all employees</td>
<td>0.925</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Dedicated efforts to create a supply chain security-focused workforce</td>
<td>0.874</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Make sure that all employees are vigilant towards supply chain security</td>
<td>0.895</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cargo safety (CS)</td>
<td>Our company improves […]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Product safety by reducing cargo theft</td>
<td>0.909</td>
<td>0.970</td>
<td>0.890</td>
</tr>
<tr>
<td></td>
<td>Product safety by reducing cargo loss</td>
<td>0.954</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Product safety by reducing cargo pilferage</td>
<td>0.961</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Product safety by reducing cargo tampering</td>
<td>0.949</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The impact of supply chain security practices

Table I. Measurement model evaluation proposed theoretical model (continued)
security. The survey used a five-point Likert scale (1 = “strongly disagree”, 5 = “strongly agree”) for supply chain security practices whereas for questions relating to the moderator and dependent variable, we used (1 = “very low extent”, 5 = “very high extent”). Items for cargo management, facility management, inventory management, and human resource management were mainly adopted from Hintsa et al. (2009), Knight (2003), Gutierrez et al. (2007), and Urciuoli (2010). Whereas for items for security culture were adopted from Voss et al. (2009), Williams et al. (2009), and Rinehart et al. (2004). Items for supply chain security operational performance were adopted from Peleg-Gillai et al. (2006), which comprised cargo safety, supply chain visibility, supply chain efficiency, and supply chain resilience.

Six experienced researchers were asked to review the questionnaire for ambiguity, clarity, and appropriateness of the items used to operationalize each construct (DeVellis, 1991). These researchers were also asked to assess the extent to which the indicators sufficiently addressed the subject area (Dillman, 1978). Based on the feedback received from these researchers, the instrument was modified to enhance the clarity and appropriateness of the measures purporting to tap the constructs. Then, the survey instrument was mailed to seven supply chain security managers. These managers were asked to review the questionnaire for structure, readability, ambiguity, and completeness. The final survey instrument incorporated feedback received from these managers, which enhanced the clarity of the instrument. Finally, the scale purification was iterative through the empirical test. This process yielded a survey instrument that was judged to exhibit high content validity.

**Analysis**

This study applies partial least squares (PLS) using SmartPLS 2.0 (Beta) M3 (Ringle et al., 2005). We then applied nonparametric bootstrapping (Efron and Tibshirani, 1993; Wetzels et al., 2009) with 5,000 replications as suggested by Hair.
et al. (2013). This technique has been used due to its appropriateness to the exploratory nature of this study where the moderating effect of security culture have not been previously tested.

The two-step approach was utilized in data analysis, as suggested by Hair et al. (2013). The first step involves the analysis of the measurement model, while the second step tests the structural relationships among the latent constructs. The two-step approach aims at establishing the reliability and validity of the measures before assessing the structural relationship of the model.

Results

Common methods variance
According to Podsakoff and Organ (1986), common method bias is problematic when a single latent variable accounts for the majority of the explained variance. The results of un-rotated factor analysis indicate that the first normalized linear combination only explains 39.54 per cent of the total 79.22 per cent variance, indicating that common method bias was not a serious problem in the study.

Measurement model results
The PLS test of the measurement model has three primary aspects: individual item reliability; internal consistency of the entire scale; and discriminant validity. Individual item reliability was assessed by examining the factor loadings of each measure on its corresponding construct. Hair et al. (2010) suggested accepting items with loadings of at least 0.6. Since the loadings associated with each of the scales were all greater than 0.6 (Table I), individual item reliability is acceptable.

The construct internal consistency was assessed using composite internal scale reliability, which is similar to Cronbach’s α. All nine latent variables satisfy the Hair et al. (2010) guidelines of at least 0.7 for internal consistency (Table I). Internal consistency can also be evaluated using the average variance extracted (AVE), which is a measure of variance accounted for by the underlying variable. The present study has an AVE of above 0.5 for all variables, satisfying the criterion of Fornell and Larcker (1981) and providing further support of the internal consistency (Table I).

We used two approaches to assess the discriminant validity of the constructs. First, we examined the cross-loading of the indicators, which revealed that no indicator loads higher on an opposing construct (Hair et al., 2012). Second, we applied the criterion of Fornell and Larcker (1981) and tested whether each construct’s AVE is greater than its squared correlation with the remaining constructs (Table II). Both analyses confirm the discriminant validity of all constructs.

<table>
<thead>
<tr>
<th></th>
<th>CM</th>
<th>CS</th>
<th>FM</th>
<th>HRM</th>
<th>IM</th>
<th>SCE</th>
<th>SCR</th>
<th>SC</th>
<th>SCV</th>
</tr>
</thead>
<tbody>
<tr>
<td>CM</td>
<td>0.839</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CS</td>
<td>0.700</td>
<td>0.943</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FM</td>
<td>0.635</td>
<td>0.631</td>
<td>0.849</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HRM</td>
<td>0.547</td>
<td>0.539</td>
<td>0.596</td>
<td>0.845</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IM</td>
<td>0.537</td>
<td>0.628</td>
<td>0.608</td>
<td>0.652</td>
<td>0.827</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SCE</td>
<td>0.580</td>
<td>0.525</td>
<td>0.508</td>
<td>0.521</td>
<td>0.522</td>
<td>0.925</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SCR</td>
<td>0.509</td>
<td>0.550</td>
<td>0.486</td>
<td>0.600</td>
<td>0.590</td>
<td>0.658</td>
<td>0.886</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SC</td>
<td>0.604</td>
<td>0.625</td>
<td>0.701</td>
<td>0.650</td>
<td>0.555</td>
<td>0.624</td>
<td>0.549</td>
<td>0.925</td>
<td></td>
</tr>
<tr>
<td>SCV</td>
<td>0.473</td>
<td>0.577</td>
<td>0.618</td>
<td>0.650</td>
<td>0.552</td>
<td>0.529</td>
<td>0.524</td>
<td>0.632</td>
<td>0.901</td>
</tr>
</tbody>
</table>

Table II. Discriminant validity coefficients
We applied the repeated indicators approach for second-order constructs on security operational performance. As suggested by Hair et al. (2013), the same measurement model evaluation criteria (with the exception of discriminant validity between second-order constructs and their particular first-order constructs) were applied to the high-order component, and the internal consistency reliability and convergent validity was established, as shown in Table III. All the lower-order constructs significantly ($p < 0.001$) affect security operational performance. The CR and the AVE of the second-order construct met the criteria for reliability and convergent validity.

Assessment of the structural model
With the satisfactory results in the measurement model, this study subsequently evaluated the structural model to confirm the relationships among constructs via the PLS method. The explanatory power of the research model was examined in terms of the total explainable variation of the model. The results suggest that the model is capable of explaining 69.9 per cent of the explainable variation on security operational performance. The effect size of $f^2$ was computed using the following formula: $f^2 = (R^2_{\text{ Included}} - R^2_{\text{ Excluded}}) / (1 - R^2_{\text{ Included}})$. The $f^2$ analysis complements $R^2$ in that the effect size of the impact of specific latent variables on the dependent latent variables can be examined (Chin, 2010). Among the security initiative practices, cargo management has the highest effect size ($f^2 = 0.146$) on security operational performance, whereas facility management has the lowest ($f^2 = 0.047$). Besides estimating the magnitude of $R^2$, researchers have recently included the predictive relevance developed by Stone (1974) and Geisser (1975), as an additional assessment of model fit. This technique represents the model adequacy to predict the manifest indicators of each latent construct. The Stone-Geisser $Q^2$ (cross-validated redundancy) was computed to examine the predictive relevance using the blindfolding procedure in PLS.

Following the guidelines suggested by Chin (2010), a $Q^2$ value of greater than zero implies that the model has predictive relevance, and, in the present study, a value of 0.384 was obtained, which is greater than zero. We applied nonparametric bootstrapping (Efron and Tibshirani, 1993; Wetzels et al., 2009) with 5,000 resamples to test the structural model. The significance and relative strength of direct effects specified by the research model were evaluated (Table III, Figure 2). The results reveal that all paths are positively significant; and, therefore, $H1$-$H4$ are supported. Our findings suggest that cargo management, facility management, human resource management, and information management collectively measured a higher order of supply chain security practices.

The product indicator approach (mean-centred) was employed to create the interaction construct (Hair et al., 2013). The CR and the AVE of the interaction constructs met the criteria for reliability and convergent validity. The results indicate that only the interaction of facility management and security culture ($\beta = 0.088$, $p < 0.05$) has a positive significant effect on security operational performance. As such, $H5b$ is supported, whereas $H5a$, $H5c$, and $H5d$ are not supported (Table IV).

<table>
<thead>
<tr>
<th>Hypothesis</th>
<th>Relationship</th>
<th>Path coefficient</th>
<th>Effect size</th>
<th>Decision</th>
</tr>
</thead>
<tbody>
<tr>
<td>$H1$</td>
<td>CM$\rightarrow$SCSOP</td>
<td>0.288***</td>
<td>0.146</td>
<td>Supported</td>
</tr>
<tr>
<td>$H2$</td>
<td>FM$\rightarrow$SCSOP</td>
<td>0.175*</td>
<td>0.047</td>
<td>Supported</td>
</tr>
<tr>
<td>$H3$</td>
<td>HRM$\rightarrow$SCSOP</td>
<td>0.269***</td>
<td>0.113</td>
<td>Supported</td>
</tr>
<tr>
<td>$H4$</td>
<td>IM$\rightarrow$SCSOP</td>
<td>0.271***</td>
<td>0.116</td>
<td>Supported</td>
</tr>
</tbody>
</table>

Table III. Path coefficients and hypothesis testing

Notes: *$p < 0.05$; ***$p < 0.001$ (one tailed)
Figure 3 illustrates that security culture strengthens the effect of facility management on security operational performance. With low security culture, high and low facility management practices have no different effect on security performance. This indicates that facility management practices are effective when the security culture is high.

**Discussion and implications**

The purpose of the present study is to identify the relationship between supply chain security practices and the security operational performance of service provider firms in the logistics industry in Malaysia and the effect of security culture on the relationships.
between security practices and the security operational performance. Our findings suggest that cargo management, facility management, human resource management, and information management have a positive and significant effect on supply chain security operational performance. Moreover, the moderating impact of security culture was only confirmed by the relationship between facility management practices and supply chain security performance.

The significant relationship between cargo management and supply chain security operational performance is in line with the studies conducted by Securitex (2008) who claimed that cargo-related incidents could negatively impact on firm performance. This result balances well with what has occurred in Malaysia over the past two decades. According to FreightWatch International (2011), Asia is rated with a moderate level of cargo theft risk; however, the same report mentions that the trend of cargo theft in Asia has shown a marked increase. Among all the countries in Asia, Malaysia and the Philippines are reported as having a higher number of cargo theft cases (FreightWatch International, 2013). Another source, the US Daily (2011), quoted that goods worth US $22.7 million (RM68.9 million) were stolen from Malaysian ports, airports, warehouses, and trucks between 2007 and 2010. Malaysia is recognized as a location for multinational companies operating their manufacturing plants for high technology products, while, at the same time, Malaysia is one of the riskiest countries in Asia with a high rate of cargo theft (FreightWatch International, 2011, 2013). Cargo theft in Malaysia occurs while the cargo is in transit and while it is stored in the warehouse. Therefore, it is not surprising that, among supply chain security practices, cargo management has the highest impact on supply chain security operation among logistics service providers in Malaysia.

Facility management is also significantly related to the supply chain security operation. This indicates that the storage areas of the cargo and products, and premises with security guards, CCTV monitoring, physical obstacles to avoid theft, proper identification of entry and exit areas, periodic inspection to ensure integrity of security measures, will improve the operational security of the logistics service providers. In addition, this study highlighted the role of the human resource management concerning supply chain operational security of logistics service providers. This result is consistent with Rice and Caniato (2003) who found that employee screening and hiring practices are important aspects of the supply chain security operation.

Figure 3.
Interaction effect of facility management and security culture on security operational performance
This proves the importance of human intervention for improving the operational security of service providers in the logistics industry. All security-related practices are carried out by the firms’ employees. Employees are the people who enforce the security practices in a firm. During the hiring process, firms’ security policies and practices will be exposed to employees during the initial stage of their employment. In order, to achieve higher operational security, firms need to hire employees who are sensitive to security issues and will not take advantage at any point of time. Employees working in the logistics firms must be trustworthy and responsible (Mayhew, 2001; Ekwall, 2009) and new employees entering the firms must go through a proper reference check by the management team (Mayhew, 2001; Ekwall, 2009) because these employees will handle cargo worth millions of dollars for which safety becomes the main priority.

Moreover, the results also showed that information management has a significant impact on supply chain operational security. This result is consistent with Michelberger and Labodi (2009), who also found a significant relation between information management and the operational security of an organization. Critical information needs to be protected and safeguarded during disruption so that firms can quickly recover to continue operation; hence, firms must have a backup system to keep information about the customer, supplier, process, procedures, and intellectual property safely. Rice and Caniato (2003) suggested having an IT system to protect data loss, setting up and operating a parallel IT system, using a range of communication tools and having a business continuity plan as preparation to respond and restore operations whenever an unexpected event takes place in the supply chain.

As mentioned by Voss et al. (2009), to ensure complete coverage of supply chain security, firms must employ both internal and external strategies. Therefore, a security culture is essential for the implementation of security initiatives and for better supply chain security operational performance. Thus, the study predicted that the existence of a security culture as a moderator would enhance the positive effects of security initiatives on the operational performance of supply chain security. The results show that security culture just moderate the relationship between facility management and the supply chain security operational performance. This result implies that, by having a stronger security culture among the employees, the effect of facility management on security operational performance will be higher. Hence, it is crucial for managers of service provider firms in the logistics industry to do the necessary work to enhance the employees vigilance towards supply chain security, to create a supply chain security-focused workplace, and make supply chain security a norm for all employees.

The reason why most of the hypotheses are not supported when the moderator is present could be because security culture is in the initial stage of implementation among supply chain service providers in Malaysia and many firms only practice internal strategies. This reason is similar to the reason that is highlighted by Rice and Caniato (2003) who stated whereby many firms attempt to practice internal strategies but only limited companies practice both of internal and external strategies. They suggest that before practicing any supply chain security initiatives, the organizational culture needs to be enhanced. The difference between the levels of security culture among logistics service providers in Malaysia is low and its moderating role cannot be captured. Therefore, for future study, the moderating role of security culture needs to be investigated in developed countries.

This study illustrates many implications for the supply chain managers and policymakers, which, if adopted, will enable supply chain firms to manage and deliver their respective customer’s products to the final destination without any disruption. The
significance of cargo management, facility management, human resource management, and information management suggests that policymakers in Malaysia should set appropriate policies and incentives to encourage businesses to adopt supply chain security practices. When properly designed, these measures can encourage firms to innovate and create new solutions to become safer and directly affect the security operational performance. In addition, the findings of this study assist supply chain managers and logistics re-examine their existing supply chain security model by considering the selected supply chain security practices, which have a significant impact on supply chain security operational performance. Managers should take security issues into account in planning organizational strategies and provide strong and consistent support to the overall security programme (Ruighaver et al., 2007) in order to create a supply chain security-focused workforce. In conclusion, individual firms need to strategize their business model with the inclusion of security aspects, which will surely create a competitive advantage over other players in the logistics industry.

This study uses RBV as a theoretical lens, to investigate supply chain security operational performance based on RBV. The study provides an empirical test of the theory in the supply chain security context. From an academic perspective, our research specially developed the concept of supply chain security operational performance by recognizing the role of resources and capabilities in security operational performance. This study has extended previous research conducted in developed countries and provides great potential by advancing the understanding between the supply chain security practices and security operational performance amongst Malaysia’s service providers in the logistic industry. This research has also contributed to the literature by examining the moderating effects of the security culture on the relationship between supply chain security practices and operational performance. To the best of our knowledge, our research is the first study to conduct such a theoretical and empirical examination.

Conclusions, limitations, and further research
As supply chains become increasingly global, firms will be forced to adopt strategies for the secure flow of goods from raw material to end consumer. Furthermore, security-related issues are frequently uppermost in the minds of many end consumers, and will require all supply chain members to take a fresh look at the security measures. In response to the importance of security issues in supply chain and the far limited discussion regarding its operational performance in developing countries, the study developed a research model and evaluated its empirical validity and explanatory usefulness by using a survey study that involved Malaysia’s service providers in the logistic industry. The study’s overall data analysis results support the research model, which showed reasonable statistical significance and classification accuracy. Moreover, findings of the study suggest that cargo management, facility management, human resource management, and information management have a significant impact on supply chain security operational performance. The results also confirmed the moderating role of security culture on the relationship between facility management practices and supply chain security performance.

There are certain limitations that need to be taken into account for generalizing the results of this study. One limitation is that, the study tested and verified the hypotheses with a questionnaire survey and only provided a cross-section of the study in nature. Therefore, it limits the ability to imply causality in the relationships among the variables. Thus, the result of the survey will be affected by the fact that this study cannot observe the dynamic change of security operational performance in the process.
of the development of supply chain security practices. As such, a longitudinal study should be attempted, that examines the relationships for an extended period of time to be able to provide more precise results. Furthermore, this study used a survey sample limited to the Malaysia’s service providers in the logistics industry. However, the effect of the security practices on operational performance and security culture might be different between countries. In addition, small firms make up a large portion of the sample that may not have formal, or the wherewithal to have formal human resource management, information management, and facility management. Thus, future research could test the research model of this study in different countries and collect data from big firms. Another limitation of this study would be the respondent firm’s customer base, which will be different for each firm. Different customer bases, such as electronic and electrical, plastic and packaging, chemical, metal, and others will present their own security concerns for their products. Therefore, different respondents serving different customer bases will have different opinions about the questionnaires forwarded to them. This study does not cover the security initiatives implemented by the government; hence, presenting a limitation and the need for a more structured study among the service providers in the logistics industry. In addition, security culture may also be an antecedent to the supply chain security practices; therefore, future studies could test the security culture as an antecedent.

References


The impact of supply chain security practices