Global Journal of Management and Business Research: a Administration and Management
Volume 17 Issue 6 Version 1.0 Year 2017
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 2249-4588 & Print ISSN: 0975-5853

Impact of Information Security Initiatives on Supply Chain Performance

By Hossam Ahmed Hanafy & Abd`Elazez Hashem
Cairo university

Abstract- *Purpose: Study aims to:*

1. Develop a comprehensive framework for the effective application of information security encompassing the internal and external technical environment, formal and informal management, and includes several aspects from an organizational perspective and between organizations in the context of the supply chain.
2. Exploring the potential outcomes and outcomes of the effective application of internal and external information security initiatives to supply chain performance.
3. Study the impact of effective application of internal and external information security initiatives on supply chain operations from the internal and inter-organizational perspective.
4. Study the impact of supply chain operations on supply chain performance. Design/ Methodology/ Approach - Based on extant information security management and supply chain security management literature, a conceptual model was developed and validated. A questionnaire survey instrument was developed and administered among supply chain managers to collect data.

Keywords: *information security initiatives, supply chain operations, supply chain performance, egyptian automotive industry.*

GJMBR-A Classification: *JEL Code: M19*

Strictly as per the compliance and regulations of:

Impact of Information Security Initiatives on Supply Chain Performance

Hossam Ahmed Hanafy [α] & Abd`Elazez Hashem [σ]

Abstract- Purpose: Study aims to:

1. Develop a comprehensive framework for the effective application of information security encompassing the internal and external technical environment, formal and informal management, and includes several aspects from an organizational perspective and between organizations in the context of the supply chain.
2. Exploring the potential outcomes and outcomes of the effective application of internal and external information security initiatives to supply chain performance.
3. Study the impact of effective application of internal and external information security initiatives on supply chain operations from the internal and inter-organizational perspective.
4. Study the impact of supply chain operations on supply chain performance.Design/Methodology/ Approach - Based on extant information security management and supply chain security management literature, a conceptual model was developed and validated. A questionnaire survey instrument was developed and administered among supply chain managers to collect data. Data was collected from 90 organizations belonging to different nodes of Egyptian automotive industry. Study employed exploratory and confirmatory factor analysis for data analysis. Further, to test the hypotheses and to fit the theoretical model, Structural equation modeling techniques were employed.

Research Findings: Results of this study indicates that:

1. Effective application of information security initiatives has a positive impact on supply chain operations. The explanatory power of supply chain operations from the effective implementation of information security initiatives is 65.3%.
   i. Effective application of internal information security initiatives has a positive impact on supply chain operations. The explanatory power of supply chain operations from the effective implementation of internal information security initiatives is 64%.
   ii. Effective application of external information security initiatives has a positive impact on supply chain operations as the interpretive capacity of supply chain operations from the effective implementation of external information security initiatives is 61.8%.
2. Supply chain processes have a positive impact on supply chain performance. Where the explanatory capacity of supply chain performance of supply chain operations is 61.5%.
3. There is no statistically significant relationship between the dimensions of effective application of internal and external information security initiatives and supply chain performance.

Problem of study: Here are many gaps highlighted by previous studies and the current study attempts to fill them will be clarified as follows:

1. Despite the importance of the exchange of information and its benefits, there are some obstacles and challenges to its success and persistence, including the concerns of the supply chain partners regarding the confidentiality and privacy of information, so a reliable network must be established so that partners share information through them . There is therefore a great need for an information security structure, where the information exchanged by organizations with the supply chain partners is one of the most important assets to them. (Kollurum and Meredith 2005; Chang et al., 2008; Qingxiong et al., 2008; Merete et al., 2008; Douglas et al., 2009; Ramesh et al., 2010; Kelly et al., 2010: Suhazimah and Ali 2012; Zahra et al 2013; Metalidou et al., 2014; Sindhuja 2014).
2. Effective application of information security initiatives includes standards, procedures, practices, culture, and information security policies and awareness creation among all employees of the Organization. And a closer look at most of the studies undertaken in the field of information security (Ashton, 2008; Werlinger et al., 2009; Douglas et al., 2009; et al., 2014; Sindhuja, 2014) we find that they have incorporated those variables within their organizational framework. However, most studies have proposed expanding research and study in the external environment of the organization as in the supply chain. (Sarathy, 2006; Voss et al., 2008; Jouini et al., 2014; Metalidou et al., 2014; Sindhuja, 2014)
3. Douglas et al. (2009) study showed that internal information security initiatives are easier to implement than external initiatives because they do not require coordination among partners. In addition, there is likely to be a learning curve for security initiatives that allows companies to start from the inside out. Where internal security is first implemented (for example, physical security initiatives are initiated) and hence the direction of external security initiatives throughout the supply chain. However, there is a major weakness in the implementation of security initiatives, which focus only on internal processes. Many researchers have mentioned that cooperation between supply chain partners is key to security success.
4. Jouini et al. (2014) study shows that nearly 71% of fraud and information fraud is committed by individuals within the organization, although 91% of security controls focus on external threats. We need to examine the effective application of both internal and external information

Author α: Teaching Assistance, Associate Professor and director of RCSC.

Author σ: Business Administration Department, Faculty of Commerce, Cairo University (EGYPT). e-mails: Hussam_ahmed@foc.cu, edu.eg

security initiatives. Most studies on information security have focused on technological, formal or informal controls (Dhillon, 2007). However, there is a need to develop a comprehensive and integrated framework for the effective application of information security initiatives that include all security controls within and between organizations (Sindhuja, 2014).

5. Ernst and Young Survey showed that the number of security incidents reported only in 2016 in the United States is only 3,720,529 security incidents, and each security incident costs the organizations $ 17-28 million. There is also an increase in the number of small and large organizations that suffer from security breaches. The number of large organizations that have been hit by security breaches reached 90%. The number of small organizations reached 74%. There is also an increase in the cost of security breaches against large organizations. Million pounds in 2014 to 3.14 million pounds in 2015, and for small organizations, the cost of security breaches increased from 115 thousand pounds in 2014 to 311 thousand pounds in 2015 (Information security beaches survey, 2015). In spite of the increased attacks and security breaches against organizations, managers often do not view the issue of information security with sufficient attention and many allow their corporate information systems to have little protection or are not protected at all. Management of information security is still insufficient. (Kelly et al., 2010).
6. Elwan and Ogunyemi (2012) study of the Egyptian garment and textile industry indicated that there are very few studies on management change in supply chain management by focusing on studying the impact of supply chain management practices on the performance of various industries. Relations between suppliers and buyers need to be further improved and developed by organizations so that they can be globally competitive, and this will be achieved by maintaining the security and confidentiality of information. The study will therefore address the effective application of internal and external information security initiatives.
7. Sindhuja study (2014) adds that there is a severe lack of scarcity in previous studies on the effective application of internal and external information security initiatives, which include the three disciplines of information security management in supply chains, and their impact on supply chain operations and performance., 2014). The study aims to examine the impact of the effective application of internal and external information security initiatives on the operations and performance of the supply chain.

The study focuses on bridging these gaps by conducting a quantitative study to study the effective application of internal and external information security initiatives and their impact on both supply chain operations and performance by applying to the chain of all the partners in the supply chain of the Egyptian automotive industry.

Originality/Value:

1. Strong competition among supply chains prevails under globalization. This study is linked to the organization's ability to effectively implement internal and external information security initiatives. In this context, study provides knowledge and quantitative analysis on how to effectively implement organizational information security management initiatives through a combination of formal and informal technical security aspects (Sindhuja, 2014).
2. The importance of study is due to the importance of its subject matter, especially in light of the lack of internal and external information security initiatives. The implementation of information security initiatives has become an urgent necessity for all business organizations. The concept of information security is now an important concept for information preservation and is the most valuable and important asset of the organization along supply chains (Akram, 2013; Sindhuja, 2014).
3. There is a lack of previous studies on internal and external information security initiatives, which include the three technical, formal and informal controls of information security management in supply chains (Sindhuja, 2014).
4. There is a great need to develop a security structure for information, where information exchanged by organizations with supply chain partners is one of the most important assets, and until the exchange of information requires organizations to make security arrangements on both sides of the transmission and reception. (Kollurum and Meredith 2005; Chang et al., 2008; Qingxiong et al., 2008; Merete et al., 2008; Douglas et al., 2009; Ramesh et al., 2010; Kelly et al., 2010; Suhazimah and Ali 2012 ; Zahra et al 2013; Metalidou et al., 2014; Sindhuja 2014).

Keywords: information security initiatives, supply chain operations, supply chain performance, egyptian automotive industry.

I. Introduction

The issue of information exchange among supply chain partners in the business environment has been a major concern in previous studies (Sindhuja, 2014).

In recent years, the environment has become more competitive than in the past. Integrated supply chain relationships are important and necessary and integral to the organization's successful structure. Supply chain management can be defined as processes and practices aimed at efficient and efficient flow of both material and information between the company, suppliers and customers (Lancaster et al., 2006). The exchange of information and communication between partners, and the potential for feedback from clients and the search for solutions to their problems, will undoubtedly have a positive impact on the organization's performance and outputs.

As Lancaster et al. (2006) note, it is necessary to adopt the supply chain for material control and information flow, and to undertake both infrastructure and infrastructure processes related to the conversion of raw materials to value-added products, and delivery of end products to customers and markets from Through appropriate distribution channels.

The common feature of supply chains today is the replacement of inventory with information provided that it is accurate and modern. Inventory management is

the most difficult part of the company's operations, due to the dynamic and changing nature of the market, making stock retention more likely to result in loss to companies as a result of the shift to idle capital, which increases the cost of the final product. When stock is replaced with information, there is a need for both planning and forecasting. Today, IT technologies have evolved and become more innovative, increasing the ability of companies to integrate supply chain parts so that products can be produced in the right quantities and distributed in a timely and cost-effective manner. This requires the need to collect the necessary information about customer preferences and to identify quantities required early for each supply chain partner so that uncertainty can be minimized (Faisal et al., 2006). Supply chain management is a complex and important issue for organizations, compete in the global market and increase customer expectations, leading to huge investment by companies in supply chain management.

With regard to the expected benefits of supply chain collaboration, the findings of Soonhong et al. (2005) show several benefits for this collaboration, including increasing supply chain capabilities, including accurate demand assessment, new skills and knowledge, there is no excess stock and no inventory at the same time. The effectiveness of the supply chain is achieved by improving responsiveness to customer requirements and improving access to targeted market segments. Companies also benefit from cooperation in developing supply chain capabilities that contribute to enhancing organizational performance, ultimately achieving competitive advantage, reducing inventory retention costs, improving customer service, increasing the quality of demand forecasting, reducing unexpected demand volume, and developing long-term relationships with Supply chain partners, contribute to the stability of operations, improve delivery and delivery of orders to customers, and make corporate systems open to enable information exchange. By doing so, supply chains become more end-user oriented. Long-term relationships achieve stability in operations, make companies more focused on their core competencies while outsourcing to meet their remaining needs, and improve customer relationships by providing the ability to anticipate, track customer demand and respond to their reactions. Customers are encouraged to identify their needs and requests, to provide efficiency and to track delivery through the ability to provide better customer service. Lancaster et al. (2006) noted that supply chain collaboration is a significant means of increasing sales, reducing supply time, achieving smaller batches, reducing stock levels, rapidly designing new products, and collaborating and coordinating supply chain members, improve corporate performance and shorten the cycle of satisfaction (Fawcett et al., 2007). The results of the Ramesh et al. (2010) study indicate that collaboration among supply chain partners has many benefits, including meeting customer needs more effectively than each company has done on its own. The Elwan and Ogunyemi study (2012) shows that the indicator that illustrates the power of communication among supply chain partners is the level of confidence, collaboration, communication and adaptation among supply chain partners. Study also examined the impact of communication and exchange of information with partners on supply chain performance in textile and garment companies in Egypt, pointing out that these companies should establish long-term partnership relations with their suppliers and customers and invest in business processes that provide them with the highest level and quality of information exchange.

The lack of awareness about the existence of obstacles prevents the achievement of the desired benefits of cooperation and information exchange. Thus, barriers to achieving cooperation in the supply chain must be identified so that decision makers can overcome these obstacles and achieve the desired benefits of cooperation in the supply chain (Ramesh et al., 2010). The information exchange across the supply chain faces many challenges, including a lack of confidence among supply chain partners. Lack of trust is the most important reason for difficulties in achieving cooperation between supply chain partners. Trust can be considered as the key factor in establishing relationships with supply chain partners, confidentiality of information exchanged, lack of strategic and cooperative planning, lack of senior management commitment, lack of clear vision and understanding of the supply chain, divergence of technological capacity among partners, inadequate exchange of information, The desire to share risks and returns, the lack of appropriate or consistent performance measures, the inaccuracy of information exchanged and the development of capabilities that allow companies to benefit from the exchange of information in a more effective manner. These constraints also have several consequences, such as lack of a clear supply chain vision, lack of competitive advantage, supply chain inflexibility, inadequate operational objectives and concerns about the privacy and confidentiality of information. A reliable network of information partners must be established. There is a great need for an information security structure. Information exchanged by organizations with supply chain partners is one of the most important assets for organizations. Until information is shared, organizations need to make security arrangements. (Kollurum and Meredith 2005; Chang et al., 2008; Qingxiong et al., 2008; Merete et al., 2008; Douglas et al., 2009; Ramesh et al., 2010; Suhazimah and Ali 2012; Zahra et al., 2013; Metalidou et al., 2014; Sindhuja 2014).

The risk of security incidents and breaches increases as a result of increased reliance on information technology, and organizations are increasingly vulnerable to various types of cyber-attacks (Jouini et al., 2014). Security breaches can cause significant financial losses, disrupt and stop operations The internalization of organizations and communications with supply chain partners, the low sales potential, the lack of competitive advantage as well as the impact on the organization's reputation. As a result, Information Security Management (ISM) has become an important and required function for all organizations. Today it is virtually impossible or impossible for organizations to operate without the effective implementation of internal and external information security initiatives with supply chain partners (Qingxiong et al., 2008). From a supply chain perspective, information exchanged between organizations and supply chain partners is among its most important assets. This calls for the need to ensure the exchange of information, communication and facilitating the flow of information. In this context, the issue of information security is a very important issue that has attracted the attention of research and practice communities in the context of current business. Information security practices have evolved from simply addressing violations and simple security breaches to managing situations facing major security threats, Organizational Perspective with a broader and more comprehensive focus, an increasing number of organizations have begun to recognize the importance of maintaining information security, identifying the relationship between security, the presence of a brand and maintaining the reputation of the organization (Sindhuja, 2014).

The information security system has evolved to serve as a wake-up call for modern organizations. The Akram (2013) study aimed to explore the impact of information security rules and regulations, management support for security awareness, security culture of work, securing internal and external communication of work, and high security efforts in organizations to maintain effective information security, Decision in organizations. Information security rules and regulations are the highest priority for effective information security. The effectiveness of information security also increases the confidentiality and integrity of partners and makes more informed decisions by managers. The John (2012) study shows that the Information Security Department enhances the protection and security of information and the continued work within and between organizations and with its partners. Business Continuity Management (BCM) also relies on recovery from technical crises and failures. IT enhances business continuity. From an economic point of view, IT reduces IT downtime and thus contributes to better financial results. Every minute of downtime has its price.

In this context, it is clear that the use of information technology to maintain information security is a prerequisite for business continuity. The term business continuity refers to the ability of the organization to perform its operations continuously even after a technical malfunction in the system, and uses many technologies and technological tools to maintain the system and prevent its failure. Therefore, many organizations seek to be more e-business oriented to select the operating systems that provide the highest levels of availability, reliability, sophistication and security of information. (Nijaz, 2006).

In today's information-based business world, all businesses rely on information technology, and business technology has become the organizational engine that drives organizations to achieve strong competitive advantages. Even if organizations can compete realistically, business must continue, not be disrupted, and more flexible. To continue business requires that, the use of information technology continuously and permanently making information constantly available. The business interruption results in lost revenues, loss of customers and loss of employment. In today's business world, a few minutes of downtime causes thousands to lose millions of dollars, so stopping the job is an unacceptable choice, underscoring the need for highly reliable information systems, availability, sophistication and security (Nijaz, 2006). The recovery from security breaches and malfunctions, and fast and reliable data access, are just a few of the demands of current business organizations. Every hour that stops working costs about $ 44,000. Graham and sharman (2003) explained that it is impossible to stop working even for one minute because the cessation of work generates bad financial effects.

Information security has become increasingly important and has become the most important issue that organizations deal with in the information age. Information has become the most important and most valuable assets owned by organizations, but at the same time it is more likely to be stolen or altered and modified, thus disrupting the information security system and negatively affecting the continuity of information. the work. Effective implementation of supply chain information security initiatives is in the coordination of personnel, processes and technology and the development of both technical, formal and informal controls of the information security system (Akram, 2013). Information security issues should be viewed from both internal and external perspectives. It is therefore necessary to examine the impact of the effective application of information security initiatives on supply chain processes from an internal and inter-organizational perspective (Sindhuja, 2014).

This study will take into account the effective application of information security initiatives across the three levels of technical, formal and informal information

systems proposed by Dhillon (2008) from the internal and external perspectives of the organization and its impact on supply chain operations and performance. The impact of supply chain operations on supply chain performance.

The objective of study is to examine the impact of information security initiatives on supply chain operations from an intra- and inter-organizational perspective. Study has taken into account the information security dimensions along the three levels of information systems -Technical, Formal and Informal, as suggested by Dhillon (2007), from an internal and external perspective of an organization. Further study will also examine the impact of security-enabled supply chain operations on supply chain performance.

Given the overarching importance of information security initiatives in the supply chain, the research tried to provide a better understanding of the related issues in a systematic manner. The literature review section explores the past researches in the area and identifies significant gaps that prompted to frame relevant research questions. Based on the research questions, a research model and associated hypotheses were developed. Further the research methodology section details on questionnaire development employing Q-sort methodology, data collection process and data analyses, using structural equation modeling techniques and interpretations thereafter. Further, the manuscript discusses the expected managerial and theoretical implications of this study.

II. Literature Review

The following are the most important previous studies related to the subject of study. Studies related to supply chain management, operations, supply chain performance and effective application of information security initiatives will be presented from the perspective of both the organization and the supply chain.

a) Information Security

Kaskanhali et al., (2003) Study presented an integrated model that regulates the relationships between organizational factors, information system, security practices, and security effectiveness of the information system. Study also explained the information security practices and the standards used in this. Analysis of the data collected from sixty-three IT managers shows that organizational factors have a significant and positive impact on security initiatives and procedures.

Study (Kaskanhali et al., 2003) agreed with the present study that it aims to maintain the security of information through the effective application of information security initiatives within organizations. Study examined the organizational factors affecting the application of information security initiatives within organizations and did not address study of the application of external information security initiatives through cooperation with the supply chain partners. The current study concerned the effective application of information security initiatives within and between the organizations and the supply chain partners both internally and externally, in addition to examining the impact of those initiatives on supply chain operations and performance.

Dhillon, (2007) Study classified information security into three levels: technical, formal and informal, as follows:

- *First, the technical level:* The information security controls consist of several defense mechanisms, including voice analysis, application of firewalls, digital signatures and other authentication protocols aimed at protecting the applications of software, devices and data that are present in computer systems.
- Second, the formal level, official controls are based on rules that determine how the technical controls that have been published are to be formed.
- Finally, the informal level of how to manage information security within the organization.

In addition to technical and formal controls, informal controls play an important role in shaping the organization's security structure. Informal controls consist of training and awareness programs aimed at making employees' behavior more conducive to maintaining information security.

The researcher has benefited from study (Dhillon, 2007) in developing a comprehensive and integrated framework for the effective application of information security initiatives incorporating all controls in a comprehensive manner within and between organizations.

Ma et al., (2008) Study presents a set of information security objectives and practices that have been derived from previous studies. The survey revealed a number of security practices to maintain information security. A questionnaire was developed to measure the extent to which information security management practices are understood. Analysis of data obtained from a security information list revealed that confidentiality, accountability, integration and availability of information Specific factors for information security objectives.

Study (Ma et al., 2008) helped the researcher to learn about the goals behind maintaining information security as well as highlighting the role of organizational culture and the awareness of employees in maintaining information security.

Ashenden (2008) Study provided an in-depth understanding of the human challenges facing the Information Security Department from an organizational perspective, linking all departments of the organization

to information security management. Study also showed that human challenges lie in the management of human, social and organizational elements in order to ensure that the Organization maximizes the benefit by combining several different resources, including organizational structure, processes and management of relations within the organization.

Ashenden (2008) highlighted the importance of the human element in maintaining the security of information. She explained that the good dealing with the human element and its awareness of the seriousness of the security breaches helps to achieve information security within the organizations and reduces the disruption of work resulting from penetration and electronic attacks. Study found that the failure of the organization to implement information security initiatives affects the organization's reputation and presents it with legal accountability.

Merete et al., (2008) Study aimed to provide an effective way to effectively implement organizational information security initiatives by combining both technical and administrative methods and methods, as well as evaluating the effectiveness of these initiatives. She explained that information security encompasses both organizational and legal aspects. Study pointed to the interest of traditional research on information security in technological aspects, so there is a great need for further studies on non-technical aspects. The aim of study is to contribute to the knowledge of organizational aspects of information security by conducting research focused on the effective implementation of organizational security initiatives.

Study found that technical and administrative security initiatives such as security policies, information security procedures and methods are the most common for the implementation of organizational information security initiatives, and that there is little interest on the part of organizations to implement information security awareness programs. More effective regulatory and operational initiatives. As a result, study showed an inverse relationship between the implementation of organizational information security initiatives and the evaluation of the effectiveness of organizational information security initiatives. Information security initiatives are implemented by initiating an information security policy, defining information security controls and controls, End creation of awareness and security. However, in terms of the effectiveness of information security measures, the creation of security awareness is more effective, followed by the identification of administrative tools and methods, the definition of procedures and controls, and finally the development of an information security policy.

Werlinger et al., (2009) Study provides a comprehensive view of the challenges faced by IT practitioners in their organizations from a human, technological and regulatory perspective.

- Human challenges are due to several reasons, including the lack of security training, security culture and lack of communication with staff on security issues.
- Regulatory challenges included risk assessment, open environments and lack of sufficient budget to maintain information security, consider security as a secondary priority, narrow schedules, business relationships with other organizations, exchange important information among supply chain partners, and support senior management.
- Technological challenges include complex systems, weak systems and applications, and lack of effective tools.

The researcher benefited from the comprehensive theory presented by study in dealing with the challenges faced by IT practitioners in order to maintain the security of information.

Metalidou et al., (2014) Study showed that awareness of information security is a key tool used to overcome security vulnerabilities. Study added that the human element and workers are often the weakest loop of information assets protection, and this vulnerability is caused by the characteristics and behavior of individual's wrong. Study showed the lack of interest in previous studies to know the impact of the human element on information security, although this element plays an important role in maintaining the security of the information of the organization. The increasing threats to information technology have made us think of new solutions that focus more on technology than human-based solutions, study said. Study pointed out that the human factor is one of the most important reasons for the weak implementation of information security initiatives by 86% followed by technological reasons.

b) Supply Chain Operations

Russell and Saldanhe, (2006) Study showed several principles for security operations - supply chain awareness, integration of supply chain information, supply chain operation with the same efficiency under different circumstances and making supply chain operational decisions, and a comprehensive review of the problems facing the global supply chain. Problems planning for disasters and crises.

Li et al., (2006) Study sought to identify the impact of supply chain management processes on achieving competitive advantage and improving organizational performance. Study aimed to develop five dimensions related to supply chain management practices (strategic partnership with suppliers- customer relationship - level of information exchange - quality exchange - delay) and test the relationship between supply chain management practice and competitive advantage and to improve the performance of the organization turned competition from competition between organizations to Competition between supply

chains. Data were collected from (196) organizations and the relationship was tested. The results indicated that a high level of supply chain management practice improves competitive advantage and improves the performance of the organization.

Zhou and Jr (2007) Study described both information exchange and integration as an effective supply chain operation through their positive impact on improving supply chain performance. The objective of this study is to study the impact of the exchange and integration of information on supply chain performance. The questionnaire list data was collected from (125) industrial companies in North America.

The results of study showed that:

- Exchange of information improves the effective practice of the supply chain.
- Dynamic supply chain has a significant positive impact on effective information exchange as well as effective practice of supply chain operations.
- The process of supply chain integration becomes more important when the level of information exchange rises.
- Both information exchange as an independent variable and supply chain integration as an intermediary variable contribute to improving supply chain performance.

By comparing Zhou and Jr (2007) with the current study, it is clear that the similarities are in trying to reach an integrated supply chain management model in industrial organizations by developing relationships among supply chain members. However, Information and knowledge of their impact on supply chain integration, and knowledge of the impact of supply chain integration on supply chain performance While the current study classified the supply chain information security initiatives into internal and external security initiatives and then identified their impact on more than one supply chain operations, Supply chain, then see the impact of those processes on supply chain performance.

Richey, (2009) Study showed that crisis management research in the supply chain is still in its early stages. Study aimed to encourage researchers to continue their research on disasters and supply chain crises.

The results of study indicated that a large part of supply chain disaster management can be done by combining three perspectives:

1. Theory of Relationship Management (Cooperation).
2. Communication theory (communication).
3. The theory of competitive values (position planning).

The researcher benefited from study in strengthening supply chain operations (supply chain disaster management) and determining the impact on supply chain performance.

Study aimed at presenting previous studies of supply chain crisis management and assisting supply chain managers in dealing with supply chain crises through a comprehensive presentation of the ways of addressing crisis situations in the supply chain.

Natarajarathinam et al., (2009) Studyhas reached a comprehensive five-dimensional framework for managing supply chain crises: sources, phases of supply chain crises, rapid response to supply chain crises, and study methods that previous studies have addressed in supply chain crises and the latter.

The researcher benefited from Natarajarathinam et al. (2009) in identifying ways to deal with supply chain crises as one of the supply chain processes that the current study is concerned with and how to deal with these crises and reduce their impact by dealing with them in a proactive approach.

Sindhuja (2014) this pilot study aimed to explore the impact of information security initiatives within the organization (internal) and between FAO and other organizations (external) on supply chain operations and performance. Study developed a conceptual model based on previous studies of supply chain management and information security management. To validate the model, a questionnaire list was developed and distributed to supply chain managers. Data were collected from 197 organizations belonging to different sectors.

The results of study indicated that information security initiatives are positively related to supply chain operations which positively affect supply chain performance.

The researcher benefited from Sindhuja (2014) in identifying the most security-oriented supply chain processes to integrate supply chain information, supply chain capacity to work efficiently in different conditions and operational decision-making, and measure the impact of these processes on supply chain performance.

c) Supply Chain Performance

Gunasekaran, (2004) Study divided supply chain management performance measures into financial measures and non-financial measures. Senior management needs financial measures to make management decisions, while minimum management and employees need operational standards for day-to-day operations.

Study provides a framework for measuring the performance of the supply chain called process and management based metrics. This framework includes the following:

- Supplier evaluation - Supply chain performance metrics at the strategic, tactical and operational levels.

- Measures at the production level: a range of products and services, utilization of production capacity and effectiveness of scheduling methods.
- Delivery performance evaluation, delivery performance evaluation metrics, total cost of distribution.
- Service and customer satisfaction metrics: Flexibility, the time it takes for a customer to inquire about the product.
- Logistics costs and supply chain costs: asset-related costs - return on investment.

Copra and Meind, (2004) Study presented a balanced approach between:

- Strategic, tactical and operational levels.
- Financial and non-financial measures. Supply chain performance can be measured at different administrative levels as follows:
- Strategic level measures affect senior management decisions, and often reflect policy verification and level of compliance with regulatory objectives.
- The tactical level addresses the allocation of resources, the measurement of actual performance and the comparison of planned performance, in order to achieve the specific results at the strategic level. These decisions affect middle managers.
- Operational level standards require more detailed data and include decisions taken by lower level managers.

The most important dimension in measuring the performance of the supply chain is the flexibility. As the uncertainty and constant change in contemporary manufacturing environments are increasing, organizations tend to improve flexibility by studying four dimensions:

1. *Flexibility of service provided to the customer:* Refers to the ability to provide services to the customer according to his requests.
2. *Flexibility of the command:* Refers to the ability to adjust the size of the command and its components during the procurement process.
3. *Site flexibility:* The ability to serve customers from alternative locations or multiple outlets.
4. *Flexible delivery time:* Means the ability to deliver delivery times consistent with the time of the client.

In order to achieve the objectives of study, the SCOR model, which describes the performance of the supply chain as efficient in the use of resources, will be used effectively to achieve the objectives of the supply chain. The Supply Chain Operations Reference (SCOR) model, developed by Supply Chain Council in 1996, is among the most widely used supply chain performance metrics among all models developed to measure the performance of the supply chain, as it (Mentzer and Konrad, 1999; Theeranuphattana, 2008; Ren, 2008; Theeranuphattana and Tag, 2008; Kurien and Qureshi, 2011; Sindhuja, 2014).

1. Provide a scientific framework that takes into consideration the performance requirements of the member organizations in the supply chain.
2. The model considers supply chain activities as a set of joint and inter-organizational processes.
3. Interested in integration and communication between the members of the supply chain.
4. The model provides management practices that produce the best performance.
5. The model is concerned with measuring the performance of the supply chain through the use of multiple dimensions including:
   a. Reliability on the supply chain SC Reliability: Produced by providing the right product in place and at the right time, packaged and packaged in the correct quantity and delivered to the right customer.
   b. Supply Chain Response SC Responsiveness: means the rapid delivery of products to customers.
   c. Flexibility Supply Chain SC Flexibility: The supply chain response to market changes in order to achieve competitive advantage and maintain.
   d. Cost of Supply Chain SC costs: Include the costs associated with the work of the supply chain.
   e. Efficient Assets: Means the effectiveness of organizations in asset management to achieve customer satisfaction.
6. The model considers the performance of the supply chain as efficient in terms of optimal utilization of resources, and effective in terms of achieving supply chain objectives.

In the next section, the theoretical foundation for the development of comprehensive framework for information security in supply chain is discussed.

III. Theoretical Framework and Hypotheses Development

Benefitting from the Russell & Saldanha (2003), study has considered supply chain operations dimensions which include operational decision-making, SC robustness and SC information integration. This study used the framework developed by SCOR (Stephan, 2001; Stewart, 1995) for measuring supply chain performance as it is found more relevant for study. The conceptual model is represented in Figure: 1.

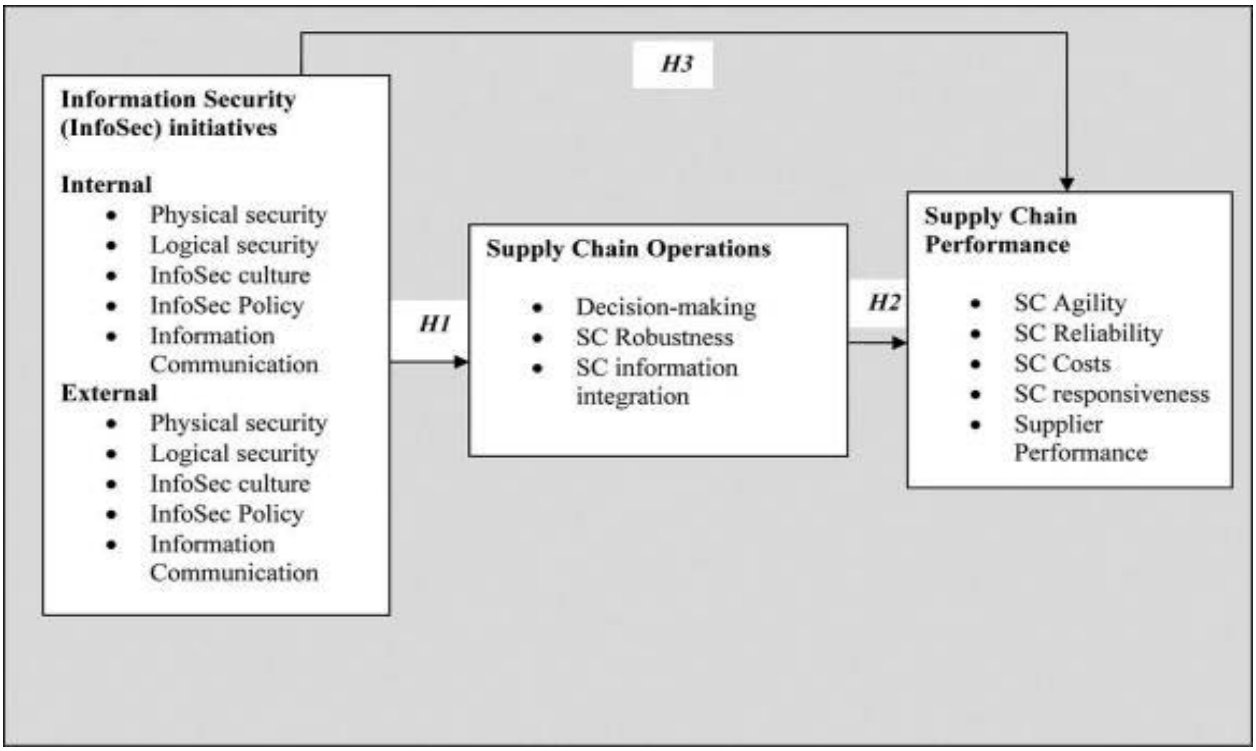

Figure 1: The conceptual model

a) Study hypothesis

In the light of study model described in Figure 1, it was possible to identify many of the relationships to be tested, which were formulated in the following assumptions:

The first main hypothesis: Effective application of information security initiatives has a positive impact on supply chain operations.

The first main assumptions is divided into two subsections:

i. Effective implementation of internal information security initiatives has a positive impact on supply chain operations.
ii. Effective application of external information security initiatives has a positive impact on supply chain operations.

Second main hypothesis: The integration of supply chain operations has a positive impact on supply chain performance.

The third main assumption:

Effective application of information security initiatives has a positive impact on supply chain performance.

The third main assumption is divided into two subsections:

i. Effective application of internal information security initiatives has a positive impact on supply chain performance.
ii. 3.2 Effective application of external information security initiatives has a positive impact on supply chain performance.

IV. Study Determinants and Applications

The limits of study include both the scientific boundaries "which are related to the methodology of study and its variants" and the practical limits "which are specific to the practical field of study," as can be seen in the following detail:

a) Scientific Limits of study

a. Study dealt with the effective implementation of internal and external information security initiatives including (physical and technical security, information security culture, information security policy, exchange of information).
b. Study focused on study of the effective application of the Egyptian automotive supply chain to internal and external information security initiatives and the impact of this on the supply chain operations which include (decision making - supply chain ability to work with the same efficiency in different circumstances - integration of supply chain information) (Which includes the most responsive supply chain - supply chain reliability - supply chain costs - supply chain response - supplier performance). As well as the impact of supply chain operations on their performance.

b) Practical Limits of study

Study was limited to companies that are located in a different contract along the supply chain of the Egyptian automobile industry. These companies are represented in:

- Manufacturers and assemblers of automotive.
- First and second tier suppliers.
- Distributors (agents ie: sales - aftermarket - spare parts).

V. Research Methodology

a) Research Sampling

The target population of this research was: All organizations in the automotive industry –throughout its three main sub-sectors– in Egypt (i.e., an example of a manufacturing industry); namely manufacturers/ assemblers of the auto feeding and automotive industries and CBU importers and distributors. A total of 101automotive firms were contacted –through email and/or phone– of which 90 accepted to participate,

b) Unit of Analysis

All the auto-feeding and automotive companies –that are operating in Egypt and implementing or partially implementing SCM practices– represented by individuals (e.g., leaders, managers and specialists) that are empowered/responsible in the area of study (e.g., SCM, ICT, and research and development (R&D) activities in these companies).

With respect to the first sector (i.e., automotive industry), probability simple random sampling technique was used as this study targeted the entire population (i.e., 101 automotive firms were contacted through email and/or phone) of which 84 accepted to participate through face-to-face depth interviews, resulting in a response rate of 89.16%. Despite being characterized by a small population size, the companies of this industry are physically dispersed at various governorates in Egypt and virtually located at different positions (i.e., multiple nodes/heterogeneous) across the same SC, which made the data collection process an extremely difficult yet value-adding one.

c) Data Collection

Primary data collected (using triangulation design) was mainly based in part ondirect/personal semi-structured in-depth interviews (qualitative data) and in part on questionnaires (quantitative data). A mixed methods approach was used in the data-collection phase to understand, map out and investigate from different standpoints (a) the research problem and proposed relationships, (b) the nature of the Egyptian automotive industry.

Study combines qualitative and quantitative approaches:

First, the researcher began to follow the qualitative approach, which depends on study and reading of data and events in a non-quantitative manner, where the data is not converted to numbers as in the case of quantitative research, but the results are obtained from the observation and analysis of events and attitudes and documents and verbal and nonverbal communication in the search, The qualitative research depends on the use of the inductive method, which is based on starting or thinking of the finished part to the whole, where the researcher starts from the data collected or observations that he observed to reach certain results (Zikmund, 2000). This means that hypotheses and theories are derived from the data set Praised the process of data collection and after analysis, the researcher examines the data here for the purpose of description and knowledge of virtual relationships between phenomena, and then returns to the community of study or place their application to collect data to test hypotheses. The qualitative research was carried out through five in-depth interviews, which helped the researcher to gain an in-depth understanding of the underlying causes of the research problem and to discover the nature of the automotive industry in the Arab Republic of Egypt.

Secondly, the quantitative part of the survey was conducted in order to measure the data collected through the questionnaire lists and then to perform quantitative statistical analysis in order to analyze and interpret quantitative data and prepare recommendations. Quantitative research aims to test the theories in a standard way, through the identification of the theory already existing in the previous literature, obtaining the necessary concepts and definitions, and then assuming the relationships between variables and data collection and analysis statistically, and in the light of the results reached by the researcher is accepted or Refusal or modification of the theory.

d) Questionnaire Development

The questionnaire list, which includes a set of terms that measure the variables of study based on the five-dimensional Likert scale, is designed to identify the impact of effective application of information security initiatives on both supply chain operations and performance. The required data have been translated into questions that help answer them in providing the necessary data for study

Measurement items used in this study were either developed from literature or adopted from previous studies. Identification and validation of newly generated items were done in two stages:

Item generation through literature review

Pilot testing using Q-sort methodology

In the first stage, potential items were generated through an extensive literature review which helped in identifying the content domain of the major constructs. This also helped in the generation of initial items and the

definition of the constructs. The initial pool of items was reviewed by academic and industry experts.

During the second phase, the items were pilot tested using Q-sort methodology (Nahm et al., 2002). The pool of items was subjected to three sorting rounds to ensure that each item was placed under right constructs.

e) Survey Administration and Sample Demographics

Transactions of credibility and consistency: The Cronbach alpha coefficient was used to measure the stability coefficient (reliability score) at the level of all variables related to the impact of the effective application of information security initiatives on the performance of the supply chain. The internal consistency coefficient of the data was also measured.

i. *Results of stability and validity tests for the dimensions of effective application of information security initiatives*

The results of the following table indicate the following:

The validity of all items at the level of the total dimensions (effective application of information security initiatives), where the internal consistency coefficients at the level of (0.01) These ranged between (0.52 to 0.91), which reflects the strength of the values of the transactions and their proximity to the correct one, The relationship between the different dimensions and the extent to which they represent the dimensions of the effective application of information security initiatives, which greatly reflects the degree of credibility of these dimensions.

With regard to sub-dimensions, the results indicate:

1. The validity of all items at the level of the total sub-dimension (effective implementation of internal information security initiatives), where the internal consistency coefficients were at the level of (0.01) and ranged between (0.52 to 0.88), which reflects the strength of the values of the transactions and their proximity to Which reflects the relationship between the different dimensions and their representation of the sub-dimension (the effective application of internal information security initiatives), which greatly reflects the degree of credibility of these dimensions.
2. The validity of all items at the level of the total sub-dimension (effective application of external information security initiatives), where the internal consistency coefficients were at the level of (0.05) and less, these ranged between (0.57 to 0.91) Approach to the correct one, reflecting the relationship between the different dimensions and the extent to which they represent the sub-dimension (the effective application of external information security initiatives), which greatly reflects the degree of credibility of these dimensions.

Based on 90 responses, all the constructs were tested for reliability, unidimensionality, convergent and divergent validity.

Information Security Initiatives (ISI), Supply Chain Operations and Supply Chain Performance Construct

ISI construct has two dimensions: Internal ISI and external ISISupply Chain Operations and Supply Chain Performance. To ensure divergent validity, a construct level exploratory factor analysis was done. All factor loading scores were above 0.7 (Hair et al., 1998).

ii. *Results of Hypothesis*

From the results, hypothesis H1 was found to be positive and significant. The impact of internal information security initiatives is greater than that of external information security initiatives on supply chain operations. This is because the Douglas, et al. (2009) study shows that internal security initiatives are easier to implement than external security initiatives because they do not require Make great efforts in coordination among supply chain partners. In addition, there is likely to be a learning curve for security initiatives, allowing companies to start from the inside out. Internal security is first implemented, for example, initiating physical security initiatives, and then progressing towards the implementation of external security initiatives throughout the supply chain. However, there is a major weakness in the implementation of security initiatives, which focus only on internal processes. Cooperation between supply chain partners is key to security success. Companies must communicate with both suppliers and customers, and cooperate with them to improve security efficiency. To achieve a competitive advantage, companies must coordinate their relationships with supply chain partners. Develop and continuously improve best security practices and share organizational knowledge through collaboration with supply chain partners. Companies that are given a low strategic security priority feel that their responsibilities will end when the product is delivered and delivered to supply chain partners. As such, companies that are given a high strategic security priority are more aware of the need for external security initiatives than companies that are given a low strategic security priority, focusing primarily on internal security measures.

Results of hypothesis 2 was also found to be significant. This is because improved supply chain management practices improve supply chain performance. In addition, this finding confirms the fact that a well-secured supply chain directly leads to enhanced and improved supply chain performance.

Results of hypothesis 3 was found to be insignificant. This indicated that information security initiatives directly cannot impact the performance of a supply chain. This indicates that direct application of information security initiatives and supply chain performance is not directly affected.

The result of this hypothesis is consistent with the results of some previous studies such as: (Sindhuja, 2014), which concluded that information security initiatives cannot directly affect the performance of the supply chain, and that there are other factors such as supply chain operations, Help improve supply chain performance.

Another logical reason for this finding is that information security initiatives are only part of the solution for the effective implementation of supply chain operations, which in turn affects the performance of the supply chain.

VI. Recommendations

In light of the researcher's compilation of the data of study and its statistical analysis and its findings, the researcher makes a number of recommendations to the managers of the supply chain of each node of the contract of the Egyptian automobile industry and the industries feeding them are as follows:

- It is possible for the managers of the Egyptian automotive supply chain to benefit from the proposed model by the researcher in trying to work on the effective implementation of internal and external information security initiatives, which improves the performance of the supply chain in general.
- Egyptian automotive supply chain managers can take care of implementing an integrated portal that combines physical and technical security to protect information assets from unauthorized access, disclosure, data modification or destruction by setting up the correct password mechanisms and keeping copies Additional and maintain network security.
- Car manufacturers and their industries should be interested in the effective application of external information security initiatives with the same degree of interest in internal information security initiatives.
- The researcher recommends the importance of maintaining security and becoming the first priority for all employees of the Egyptian automobile industry.
- The researcher is encouraged to use notices, posters and corporate newsletters to promote awareness of the information security policy.
- The interest of the Egyptian automakers in exchanging information that helps to plan business between their departments in order to maintain their competitiveness and profitability in the long term.
- The researcher recommends that the formulation of the information security policy should be characterized by an understanding of the employees and their applicability through the organization of organizations for workshops aimed at increasing the security knowledge of their employees and ensuring that all are aware of security policies and procedures.
- Need to share information among the supply chain partners about each partner's core and important processes.
- The need for each manager of the supply chain managers to be interested in integrating with other supply chain partners.
- The need for a written and documented plan for the recovery of systems, data and communications after the security problems experienced by the supply chain and its return to work normally as soon as possible.
- The supply chain needs to benefit from the different competencies of partners in order to achieve rapid response to changes in the market.
- The researcher is recommended to take care of the supply chain managers by increasing the rate of saturation of applications.
- The importance of supplying the automotive industry partners with high quality delivery.
- The need to reduce the supply chain system for both incoming and outgoing costs.

VII. Future Scope

The researcher proposes the following axes to guide them as areas for future research:

- Study the impact and interaction of several variables such as the size of the organization, the structure of the organization and the complexity of information technology in the application of information security practices between organizations.
- Study the impact of the educational level and the age of supply chain managers on the extent to which they accept the application of internal and external information security initiatives.
- Study the impact of the effective application of internal and external information security initiatives in various industries and supply chains to reach more reliable results.
- Study the impact of the effective application of internal and external information security initiatives to companies working in other industrial sectors and companies that have worked in the service sector and to know the impact on supply chain performance.

References Références Referencias

1. Ashenden, D. (2008), "Information security management: a human challenge", *Information Security Technical Report*, Vol. 13 No. 4, pp. 195-201.
2. Akram, K. (2013), "Evaluating the impact of information security on enhancing the business decision-making process" *World Journal of*

Entrepreneurship, Management and Sustainable Development, Vol.9 No.1, pp. 44-64.
3. Chang, S.E. and Ho, C.B. (2006), "Organizational factors to the effectiveness of implementing information security management", *Industrial Management and Data Security*, Vol. 106 No. 3, pp. 345-361.
4. Chang, S.E. and Lin, C. (2007), "Exploring organizational culture for information security management", *Industrial Management and Data Systems*, Vol. 107 No. 3, pp. 438-458.
5. Chen, C.C., Medlin, B.D. and Shaw, R.S. (2008), "A cross-cultural investigation of situational information security awareness programs", *Information Management and Computer Security*, Vol. 16 No. 4, pp. 360-376.
6. Cohen, J. (1960), "A coefficient of agreement for nominal scales", *Educational and Psychological Measurement*, Vol. 20 No. 1, pp. 37-46.
7. Dhillon, G. (2007), *Principles of Information Systems Security: Text and Cases*, John Wiley and Sons, New York, NY.
8. Dlamini, M.T., Eloff, J.H.P. and Eloff, M.M. (2009), "Information security: the moving target", *Computers and Security*, Vol. 28 Nos 3/4, pp. 189-198.
9. Douglas, M., Judith, W and David, C, (2009), "The role of strategic security: Internal and external security measures with security performance implications, *Transportation Journal*, Vol.48, No.2, pp. 5-23.
10. Ernst and Young Survey (2008), *Global Information Security Survey 2008*, Ernst and Young LLP, London.
11. Elwan, S. and Ogunyemi, O. (2012), "The effect of linkages and information sharing on supply chain and export performance an empirical study of Egyptian. Textile manufacturers" *Journal of Manufacturing Technology Management*, Vol.23 No.4, pp.441-463.
12. Faisal, M. N., Banwet, D. K., & Shankar, R. (2006). Supply chain risk mitigation: modelling the enablers. *Business Process Management Journal*, Vol.12 No.4, pp. 535-52.
13. Fawcett, S., Osterhaus, P., Magnanm, G. and Brau, G. (2007), Information sharing and supply chain performance: the role of connectivity and willingness. *Supply Chain Management: An International Journal,* Vol.12 No.5, pp. 358-368.
14. Fulford, H. and Doherty, N.F. (2003), "The application of information security policies in large UK-based organizations: an exploratory investigation", *Information Management and Computer Security*, Vol. 11 No. 3, pp. 106-114.
15. Gunasekaran, A., (2004), "A framework for supply chain performance measurement", *International Journal of Production Economics*, Vol. 87 No. 3, pp-333-347.
16. Hagen, J.M., Albrechtsen, E. and Hovden, J. (2008), "Implementation and effectiveness of organizational information security measures", *Information Management and Computer Security*, Vol. 16 No. 4, pp. 377-397.
17. Hair, J.F. and Anderson, R.E. (1995), *Multivariate Data Analysis*, Prentice Hall, Upper Saddle River, NJ. Johna, J. (2012), "Information security and business continuity management in inter organizational IT relationships", *Information Management & Computer Security*, Vol.20 No.5, pp.332-349.
18. Jouini, M., Rabai, L., and Aissa, A. (2014), "Classification of security threats in information systems" *Procedia Computer Science*, Vol.32, pp. 489 – 596.
19. Kankanhalli, A., Teo, H.-H., Tan, B.C. and Wei, K.-K. (2003), "An integrative study of information systems security effectiveness", *International Journal of Information Management*, Vol. 23No. 2, pp. 139-154.
20. Kolluru, R., and Meredith, P. (2005). Security and trust management in supply chains. *Information Management and Computer Security,* Vol.9 No.5, pp. 233-236.
21. Kritzinger, E. and Smith, E. (2008), "Information security management: an information security retrieval and awareness model for industry", *Computers and Security*, Vol. 27 Nos 5/6, pp. 224-231.
22. Lancaster, S., Yen, D.C., Ku, C.Y. (2006) E-supply chain management: an evaluation of current web initiatives, *Information Management & Computer Security*, Vol. 14 No.2, pp. 167-184.
23. Lee, S.M., Luthans, F. and Olson, D.L. (1982), "A management science approach to contingency models of organizational structure", *Academy of Management Journal*, Vol. 25 No. 3, pp. 553-566.
24. Li, S., Rao, S.S., Ragu-Nathan, T.S. and Ragu-Nathan, B. (2005), "Development and validation of a measurement instrument for studying supply chain management practices", *Journal of Operations Management*, Vol. 23.
25. Li, S., Ragu-Nathan, B., Ragu-Nathan, T.S., and Rao, S. S. (2006), "The impact of supply chain management practices on competitive advantage and organizational performance". *Omega*, Vol.34 No.2, pp. 107–124.
26. Ma, Q., Johnston, A.C. and Pearson, J.M. (2008), "Implementation security management objectives and practices: a parsimonious framework", *Information Management and Computer Security*, Vol. 16 No. 3, pp. 251-270.
27. Malhotra, A., Gosain, S. and El Sawy, O.A. (2005), "Absorptive capacity configurations in supply chains: gearing for partner-enabled market

knowledge creation", *MIS Quarterly*, Vol. 29No. 1, pp. 145-187.
28. Merete, J., Erik, A., and Hovden, J., (2008), "Implementation and effectiveness of organizational information security measures", *Information Management & Computer Security,* Vol.16 No.4, pp.373-397.
29. Metalidou, E., Marinagi, C., Trivella, P., Eberhagerm N., Kourlas, C., and Kopoulos, G. (2014), "The human factor of information security, unintentional damage perspective", *Procedia-Social and Behavioral Science,* Vol.147, pp. 424-428.
30. Michelberger, P. and Labodi, C. (2009), "Development of information security management systemat the members of the supply chain", *Annals of the University of Petrosani, Economics*, Vol. 9 No. 4, pp. 69-78.
31. Nijaz, B. (2006), "Information technologies for business continuity: an implementation framework", *Information Management & Computer Security*, Vol.14 No.5 pp.450-466.
32. Qingxiong, M., Johnston, J., and Micheal, P., (2008), "Information security management objectives and practices: a parsimonious framework", *Information Management & Computer Security*, Vol.16 No.3, pp. 251-270.
33. Ramesh, A., Banwet, D., and Shanker, R., (2010), "Modeling the barriers of supply chain collaboration", *Journal of Modelling in Management*, Vol.5 No.2, pp. 176-193.
34. Ratnasingham, P. and Kumar, K. (2000), "Trading partner trust in electronic commerce participation", in *Proceedings of the Twenty First International Conference on Information Systems*, Association for Information Systems, Atlanta, GA.
35. Rice, J. and Caniato, F. (2003), "Building a secure and resilient supply network", *Supply chain management review*, Vol. 7 No. 5, pp. 22-30
36. Richey, R.G. Jr. (2009), "The supply chain crisis and disaster pyramid: A theoretical framework for understanding preparedness and recovery", *International Journal of Physical Distribution & Logistics Management*, Vol.39 Issue: 7, pp. 619-628.
37. Russell, D.M. and Saldanha, J.P. (2003), "Five tenets of security-aware logistics and supply chainoperation", *Transportation Journal*, Vol. 42 No. 4, pp. 44-54.
38. Sarathy, R. (2006), "Security and the global supply chain", *Transportation Journal*, Vol. 45 No. 4, pp. 29-52.
39. Sindhuja P.N, (2014), "Impact of information security initiatives on supply chain performance". *Information Management & Computer Security,* Vol. 22 No 5, pp. 450-473.
40. Stephens, S. (2001), "The supply chain council and the supply chain operations reference (SCOR) model: integrating processes, performance measurements, technology and best practice", *Annals of the Logistic Spectrum*, Vol. 34, pp. 16-18.
41. Soonhong, S., Roath, J., Daugherty, E., Genchev, R., and Glenn, R., (2005) "Supply chain collaboration: What's happening?" *The International Journal of Logistics Management*, Vol.16 No.2, pp. 237-256.
42. Suhazimah, D., and Ali, Z.m (2012),'Assessment of information security maturity", *Journal of Systems and Information Technology*, Vol.14 No.1, pp. 23-57.
43. Tan, F.B. and Hunter, M.G. (2002), "The repertory grid technique: a method for study of cognition in information systems", *MIS Quarterly*, Vol. 26 No. 1, pp. 39-57.
44. Theeranuphattana, A. and Tang, J.C.S. (2008), "A conceptual model of performance measurement for supply chains: Alternate considerations". *Journal of Manufacturing Technology Management*, Vol.19 No.1, pp. 125–148.
45. Voss, M.D., Whipple, J.M. and Closs, D.J. (2008), "The role of strategic security: internal and external security measures with security performance implications", *Transportation Journal*, Vol. 28 No. 2, pp. 5-23.
46. Werlinger, R., Hawkey, K. and Beznosov, K. (2009), "An integrated view of human, organizational and technological challenges of IT security management", *Information management and Computer Security*, Vol. 17 No. 1, pp. 4-19.
47. Williams, Z., Leug, E.J., Taylor, R.D. and Cook, R.L. (2009), "Why all the changes? An institutional theory approach to exploring the drivers of supply chain security (SCS)", *International Journal of Physical Distribution and Logistics Management*, Vol. 39 No. 7, pp. 595-618.
48. Wilson, M. and Hash, J. (2003), "Building an Information Technology Security awareness and Training Program". *National Institute of Science and Technology*. Special publication 800-50.
49. Yu, M., Ting, S. and Chen, C. (2010), "Evaluating the cross-efficiency of information sharing in supply chains", *Expert Systems with Applications*, Vol. 37 No. 4, pp. 2891-2897.v
50. Zahra, L., Mukhtar,M., Sahran, S., and Zadeh, A. (2013), "Information Sharing in Supply Chain Management", *Procedia Technology*, Vol.11. pp. 298-304.
51. Zhou, H. and Bentor, W.C. Jr (2007), "Supply chain practice and information sharing", *Journal of Operations Management*, Vol. 25 No. 6, pp. 1348-1365.