INFORMATION SECURITY ISSUES IN GLOBAL SUPPLY CHAIN

Kamal Nayan Agarwal, Ph.D.
Howard University, USA
kagarwal@howard.edu

Ann-Marie Waterman
Howard University, USA

Abstract

In our global community, multinationals or conglomerates alike must utilize information flow to produce effective, efficient, and profitable services and products. Using a global supply chain system affords multinational corporations and other supply chain partners to achieve efficiencies and increased revenue otherwise unattainable. A consequence of these complex delivery operations and logistic schema is the management of information and sustaining its security. Sharing data across supply chain partners results in managing data security, technology, and other management issues to reduce leaks and breaches.

Keywords: Information Security, Global Supply Chain Management, Risk Management,

INTRODUCTION

As early as 2004, Closs and McGarrell defined security in supply chains as “the application of policies, procedures, and technology to protect supply chain assets … from theft, damage, or terrorism, and to prevent the introduction of unauthorized contraband, people or weapons of mass destruction into the supply chain” (Roy & Kundu, 2012, p. 305-1). A decade later, the industry becomes self-incubated, producing new market models and procedures based on technology’s demand for specific supply chain changes and issues of operation. As such, the world’s global supply chain is a constantly evolving entity that requires persistent innovation and sustainability to counter its information technology challenges. Amongst these challenges, the greatest threat to supply chain sovereignty may be security. A common target of Internet campaigns is the intellectual properties associated with the operations and the vendor specific polices and custom applications. (Ashford, 2015) Credit card user breeches and email malware have led to thousands of consumer’s personal data released on world hack sites and piracy platforms, making an individual’s financial security tentative and exposed.

Faced with the challenge of identifying who is actually inside the supply chain, it becomes nearly impossible to install effective procedures that will dissuade all pirating strategies or overcome and reject all malicious operations attempts, as threats can be physical or virtual. Physical threats include environmental disasters, theft, man-made accidents, and intentional cyber campaigns. Virtual attacks include ransom-ware wars, port denial schemas, and password phishing. Server attacks and network intrusion are threats usually attributable to international transportation, storage resources, communications and wide area infrastructures. Therefore, organizational concerns include: “Poor information security practices by lower-tier suppliers; compromised software or hardware purchased from suppliers; software security vulnerabilities in supply chain management or supplier systems; counterfeit hardware or hardware with embedded malware; or third party data storage or data aggregators” (NIST, 2015, p. 1).

Consequently, Supply Chain Information Security (SCIS) is critical for the operation of the global supply chain’s business cycles and serves as the company’s strategic framework as well as the foundation for the primary issues associated with information security. Specific issues are namely: Infrastructure and Wise Area Networks (WAN) issues; Development scopes/parameters and their respective methodologies; Intra-Operations and Protocols; Innovation Insertion and Dynamic Technologies exploitation potential, and Company Super-powers and Admin control. Conversely, It is important to note, information security objectives for supply chains, regional, national or global are simple. The objectives are: (1) To execute the transportation of the global product using a sustainable and effective operation; (2) To build a commercial supply chain that can withstand constant, persistent, dynamic threats of cyber origins; and, (3) To be able to restore operations with minimal loss of time, product, labor and profit. This paper will discuss how these protocols are effectively actualized in the global supply chain.

LITERATURE REVIEW

Stefansson (2002) stated that companies that were going to work together to be efficient and productive powers of their respective industries, they would need systems that supported proprietary as well as shared data. This revelation prompted research into the data security issues that would invariably arise when information is shared across departments, companies, and the global marketplace. Furthering that discussion, Dynes, et al. (2005) shared what seems rather obvious in present-day: in order for a supply chain to be effective, all companies must have access to the information that will increase the efficient production and timely delivery of the product from the manufacturing stage to the delivery point. Supply chain partners customarily have large volumes of data, so it is no surprise that they are susceptible to information security breaches because of the high financial reward paid to the attacker on the black market. Unger and Goel (2007) joined the discussion regarding sharing of data across the supply chain by adding their considerations about the internal and external weaknesses related to information security. They examined loss of proprietary information, system malfunction, and compromised bidding systems. Kaur et al. (2008) introduced a potential solution to these threats when they interjected that organizations should tighten their security by creating strong information policies that organizations within the supply chain all utilized.

In 2009, Anand and Goyal examined the endogeneity of information endowment. Their research indicated that while organizations would like to focus their efforts on one stage or another of the information exchange and security protocols of the supply chain, it is critical that organizations have a comprehensive strategic information management plan to examine their own and their suppliers' hard (materials) and soft (internal employee) protocols. That is, it is equally important for an organization to mange its material flows as well as its information. Using algebraic equations to quantify the exchange of information between firms and customers, and introducing the prevailing market demands, their study demonstrated that information and material flows were intertwined. Further, their research results revealed that the level of demand uncertainty is a key factor in the prevention of information leaks. They posit that though supply chain managers indicated that information leakage is one of the greatest threats (supplychainaccess.com), to supply chain operations, information leakage is challenging to eradicate because effective and efficient business operations are built and depend on information exchange, and the information is susceptible to theft. Zhang, et al. (2010) shared similar views. They purported that confidential information could be mistakenly (not intentionally)shared between supply chain partners, which could result in direct information leakage. Roy and Kundu (2012) underscored the concern and importance of information and the associated processes, systems and network to an organization, and how the breach of such information damages the organization's reputation for future business and real-time business transactions.

The next year, *Supply Chain Information Risk Management Model in Make-to-Order* (2013), written just four years later by Malaysian scholars, proffered that if a firm invested in the creation of a make-to-order information risk management model, the resulting effect would be a well-informed manager who had the tools to craft appropriate solutions and even anticipate or factor into decision making variables of potential mitigating problems in anticipation and preparation for negative impact on the supply chain.. The research team developed a model based on eight categories of information (i.e., Inventory Level; Sales Data; Order Status; Transportation/Shipment Sizes; Delivery Schedule; Sales Forecasting; Machine Capacity; and Production Schedules); 12 risk factories in information sharing (i.e., Uncertainties in demand; Inaccuracies demand data; Changes in ordering contract; Natural disasters; Late payment; Uncertainties in supply; Inaccuracies the past demand data; Machine problem; Inaccuracies of supplier data; Price fluctuation; Shipment and delivery accuracy; and Networking system problem; and, five mitigating activities (i.e., Good practice standards; Plan, Do, Check, Act (PDCA); Monitor and review protection failures; Make data backup; and Focus on information technology). (Mukhtar & Shukor, 2013) "They identified categories of information sharing, the information risks factors and the mitigation activities are then molded into make to order information risk model" (Sentia, Mukhtar & Shukor, 2013, p. 406). The research is heavily questionnaire- and panelists-based, with outcomes revealing the potentially corrective action to mitigate risks. For example, in one set of raw data, the results indicated that "in sharing inventory level information…the risks involved were uncertainties in demand, inaccuracies demand data, and uncertainty in supply. To mitigate these risks, the model suggests that (organizations should) make back up data, focus on information technology and PDCA" (Mukhtar & Shukor, 2013, p. 408).

Other researchers looked at technology aspects or information security as well as management aspects. Early technology aspects researchers indicated that practitioners were overlooking low-hanging-fruit solutions to resolve the technology matter at hand. They surmised that deficiency in the design and implementation of IT systems was the first challenge (Gunasekeran & Nigel, 2004); the improvement of customers service and satisfaction was another challenge which had given way to greater vulnerability to hackers, malware, and other unauthorized access into private networks (Smith, et al., 2008); Meanwhile, Wadhwa (2009) created a security model to retain confidentiality, authentication, and availability, whilst e-commerce brought in additional concerns about deployment, countermeasures and associated risks (Shaifinia, 2009; Ajayi & Maharaj, 2010). Finally, researchers interested in the management aspects of technology focused their concerns on the people-created side of the risk factors (Knight, 2003; Faisal, et al., 2006; Wadhwa & Saxena 2005).

METHODOLOGY

This paper will duplicate the methodology used by Roy and Kundu (2013), when they "proposed a Process Framework for the management of information security" (p. 305-1). In their study, they assessed the effectiveness of applied controls to the potential risks and possible risk management controls for different security areas: physical security, human resource security, and technology security. They then used performance indicators and an assessment process to evaluate effectiveness. In this paper, the use of Process Framework methodology will inform, educate, and encourage information technology managers to see the usefulness and strength that can be derived from the inclusion of other risk officers to create, execute, and sustain solid, information security across and throughout the global supply chain.

ANALYSIS

Research executed in 2013, revealed that 93% of large companies – 87% small businesses – were subject to security intrusions of some type. Most occurrences were data breeches, which in turn, externally exposed personal data of consumers, but internally damaged the company's infrastructure, WANs, and resulted in compromised communications routes. While predetermined outcomes, elicit prescribed actions, when it comes to supply chain security, some of these actions have little to do with the hard core decision processes of the administration or decision making tier that is prone to default to an unsynchronized response and an ineffective defense and compromised response to reign in aggressive intent. For example, in 2014 and 2017, Kmart (Sears Holdings, parent company) battled security breaches as a result of malware-based attacks on its credit-card processing systems. The virus had gone undetected by their anti-virus systems and application controls. Although no identifying data (i.e., names, addresses, social security numbers, etc.) was obtained by the attackers, some cardholder data was retrieved as the attackers sought the data to make counterfeit cards.

As attackers become more sophisticated in their threat attempts, a new term has entered the information security lexicon, Advance Persistent Threats (APT). These threats commonly attack supply chain entities because they, by definition and structure, share the most valuable information, have the most external interactions with the global market, and have the most exposure to weakness. Colin Tankard (2011) stated that the estimated costs to the UK is figured to be approximately £27bn per year and, according to some estimates, the global cost is $1trillion every year" (p. 16).

Groups of cyber-offensive nationals have recently focused on energy companies and their subsidiaries through Industrial Control Software (ICS), by the addition of malware and Trojan coding. These threats have the capacity to supersede operational control and management. Bearing in mind that information security attackers' ultimate goals are to gain control of core information, such as intellectual, or copyrighted properties, supply chain routings, distribution schema, by hijacking passwords and ultimate access to secure data. A new trend finds that the common depositories to which companies outsource data and database storage are often infiltrated by organizations that gain access to critical data and SQL archives that reveal pertinent business credentials, from credit card information to business marketing strategies and secrets. Simply stated, companies use remote database housing to store data offsite. Oftentimes, the hosting company is hacked and by default, so is the original companies' critical data, including credit card information and other company logistical data. Other forms of attack include malware ticks on company websites that are routinely downloaded by customers under the assumption they are safe, when, in fact, these ticks are unsafe. They provide intruders direct access to intimate files within the individual user's PC and a gateway to any information that is housed associated network.

Agencies such as the Payment Card Industry Data Security Standard (PCI DSS) are compliance entities that help strengthen vetting and validation by establishing standards and requirements (12.8.5 and 12.9). Because supply chains are defaulted to be friendly to in the field requirements and standards, they are open to new technology's hardware and applications that grant ordinary improvements demagogue status. This in turn, opens the supply chain to its vendors' flaws and exploited backdoors. Lackadaisical security policies – or lack of – are one of the biggest culprits, making the organization a victim of itself. Not well thought of control and laptop protocols are redirected to remote sites to be interrogated for valuable Enterprise Resource Planning (ERP) reports and Strategic Framework overviews – the company's essential hierarchy of execution.

The Advent of Physical Attacks

When 9/11 occurred, the automotive industry nearly came to a halt as the raw materials to build cars and trucks became sparse due to increased security at American boarders. Several companies' assembly lines became idle when electronics were not delivered form Europe and worldwide suppliers. When 'Just-In-Time' resources dried up, it became nearly impossible to complete vehicles for inventory and sales. These supply chain failures were not caused by information 'attacks' they were reflective of the 'information' by the government to counter physical intrusions. It also became clear that the information regarding the operational aspects of the supply chain itself was not protected and easily accessed and manipulated.

Sustainability of Information Infrastructure

Using local resources in collaboration with sustainability framework policy, procedures that address network 'lockdown' compliancy must be enacted. Further, Networks switches and routers must be protected from common 'spoofing,' 'Port Denial' and TCP/IP holes throughout company domains.

Backup

Essential for Corporate operations is the maintenance of its information. It is imperative that information security is also inclusive of information backup and restoration procedures. In the event of an information breech, daily operation effectiveness of the supply chain must be maintained and seamless. The operations of security must be compliant with the corporation established – not by technology.

While the US has become more aware of information security challenges and has incorporated protocols to lessen the threats, other governments are also addressing these issues in their regions. In 2014, the United Kingdom government required all IT suppliers to comply with Cyber Essentials Scheme (CES). CES was the European response to raise the cyber security bar for its businesses by implementing a set of basic technical controls for organizations to utilize. (Ashford, 2015). Using incentives for participation, the UK inspired technical controls afforded organizations the opportunity to gain one of two cyber essential badges. Starting October 2014, all contractors that have access to sensitive or personal information in their transactions as prescribed in their contracts, must be certified CES organizations. (Cyber Essentials, 2014)

CONCLUSION

There is a dire need to integrate security and supply chain information management interdisciplinary technologies within the global business framework. The criteria for security stratagems to protect hardware, software and firmware components of supply chain information infrastructure is necessary for business corporations to operate in today's international industries. Ever since 9/11, the global supply chain has expected the new reality: there will be attacks on supply chain security. In short, attacks are the norm. The issues and deficits faced by supply chain information networks will be ongoing, dynamic and innovative by definition – changing to match technology and the procedures that protect the product. These security intrusions and assaults on information breakdown into two arenas: (1) The environment of the supply chain after an attack; and, (2) Business Operations under new security information protocols and increased security measures.

Much like universities have adopted chief information officers (CIOs) to deal with specific grey areas that lie between academia and technology, the supply chain information entities have had to respond to the merger of supply chain information security execution and physical measures execution - whereas secure strategies (digital and physical) become business shared-disciplines executed through dissonance methodologies. These solutions which are the product of all levels of the supply chain are touched by all providing better responses, by providing a better understanding of vendors, product, supply, and transport operations. These new interdisciplinary security target future security threats and developing cyber-vision attacks are responsible for wide area intrusions and information compromises.

REFERENCES

Ajayi, N. & Maharaj, M. (2010). Mitigating information risk within supply chains. Proceedings of the International Research Symposium in Service Management, Mauritius.

American Productivity & Quality Centre. (2011). Using Process Frameworks and Reference Models: to get real work done. APQC Best Practices Report.

Anand, K. S. and Goyal, M. **(**2009). Strategic Information Management under Leakage in a Supply Chain. *Management Science*, *55*(3), 438-452.

Ashford, W. (2015, March 27). Supply chain an important part of information security, say experts. *ComputerWeekly.com*. Retrieved from: http://www.computerweekly.com/news/4500243250/Supply-chain-an-important-part-of-information-security-say-experts

Bolhari, A. **(**2009). Electronic-Supply chain information security: A framework for information security in e-SCM (e-SCIS). Proceedings of the 7th Australian Information Security Management Conference, Perth.

Closs, D. J. & McGarrell, E. F. (2004). Enhancing security throughout the supply chain. Special Report by the IBM Center for the Business of Government.

Cyber Essentials. (2015). Cyber essentials scheme: Assurance framework. His Majesty's Government.

Dynes, S., Brechbühl, H., & Johnson, M. E. **(**2005). Information security in the extended enterprise: Some initial results from a field study of an industrial firm. Report supported in part by a grant from the World Bank and in part under an award number 2000-DT-CX-K001 from the Office for Domestic Preparedness, Department of Homeland Security.

Faisal, M. N., Banwet, D. K., & Shankar, R. (2006). Supply chain risk mitigation: Modeling the enablers. *Business Process Management Journal*, *12*(4), 535-552.

Gunasekaran, A. & Ngai E. W. T. (2004). Information systems in supply chain integration and management. *European Journal of Operations Research*, *159*, 269-295.

Johnson, M. E. **(**2008). Information risk of inadvertent disclosure: An analysis of file-sharing risk in the financial supply chain. *Journal of Management Information Systems 25*(2), 97–123.

Kaur, A., Kanda, A., & Deshmukh, S. G. (2008). Supply chain coordination: Perspectives, empirical studies and research directions. *International Journal of Production Economics, 115*(2), 316-335.

Knight, P. (2003). Supply chain security guidelines. IBM Report presenting a summary of supply chain security guidelines published by numerous sources.

Motwani, J., Madan, M. & Gunasekaran, A. (2000). Information technology in managing global supply chains.

*Logistics Information Management, (13)*5, 320-327. Retrieved from: https://doi.org/10.1108/09576050010378540

National Institute of Standards and Technology (NIST). 2015. Best Practices in Cyber Supply Chain Risk Management. U.S. Department of Commerce, Workshop Brief. Retrieved from: http://csrc.nist.gov/scrm/documents/briefings/Workshop-Brief-on-Cyber-Supply-Chain-Best-Practices.pdf

O'Marah, K. O. (2017, Jan. 12). Hacked to death: Data security in supply chain. *Forbes.* Retrieved from: https://www.forbes.com/sites/kevinomarah/2017/01/12/hacked-to-death-data-security-in-supply-chain/#255b9d663c28

Poirier, C. & Bauer, M. (2000). E-supply chain: Using the Internet to revolutionize your business. Berrett-Keohler Publishers, San Francisco: CA.

Roy, A. & Kundu, A. (2012). Management of information security in supply chains: A process framework. Proceedings from the CIE42 Conference, South Africa. Retrieved from: http://www.academia.edu/1907440/Management_of_information_security_in_supply_chains_A_process_framework?token=5a5518178eeb4e11b12bb038a8df99d4

Sentia, P. D., Mukhtar, M., & Shukor, S. A. (2013). Supply Chain Information Risk Management Model in make-to-order (MTO). Proceedings of the Fourth International Conference on Electrical Engineering and Informatics (ICEEI 2013), Malaysia.

Sharifnia, M., Iranmehr, A. & Duroodochi, M. (2009). Development of trust model for e-supply chain management. Proceedings of the European and Mediterranean Conference on Information Systems, Izmir.

Smith, G. E., Watson, K. J., & Baker, W. H. (2008). Perception and reality: An introspective study on supply chain information security risk. *Issues in Information Systems, 9*(2), 272-278.

Soni, U. & Jain, V. (2011). Minimizing the vulnerabilities of supply chain: A new framework for enhancing the resilience. Proceedings of the IEEE International Conference on Industrial Engineering and Management, Singapore.

Stefansson, G. (2002). Business-to-business data sharing: A source for integration of supply chains. *International Journal of Production Economics*, *75*(1), 135-146.

Supply Chain Council. (2010). Supply chain operations reference (SCOR®) model overview - Version 10.0.

Tankard, C. (2011). Advanced persistent threats and how to monitor and deter them. *Network Security*, *2011*(8), 16-19.

Supply Chain Security Management - What Is It? Definition ... (n.d.). Retrieved from https://www.kbmanage.com/concept/supply-chain-security-management on September 11, 2017.

The Cyber Security Of Supply Chains: Who's The Real Risk ... (n.d.). Retrieved from https://medium.com/@KodiakRating/the-cyber-security-of-supply-chains-whos-the-re

Unger, D. & Goel, R. (2007). Sharing and guarding information: Managing data security in supply chain networks. *Alliance Journal of Business Research, 3*(1), 49-60.

Wadhwa, S., Prakash, A., Deshmukh, S. G., & Wadhwa, B. (2009). Information security in flexible supply chain network: A decision information security (DIS) model. *Global Journal of Enterprise Information System, (1)*2, 25-31.

Wadhwa, S. & Saxena, A. (2005). Knowledge management based supply chain: An evolution perspective. *Global Journal of e-Business and Knowledge Management, 2*(2), 13-29.

Zhang, D.Y., Zeng, Y., Wang, L., and Geng, Y. (2011). Modeling and evaluating information leakage caused by inferences in supply chains. *Computers in Industry, (62)*3, 351-363.