RAIS RESEARCH ASSOCIATION for INTERDISCIPLINARY STUDIES
August 2021

DOI: 10.5281/zenodo.5506908

Supply Chain Risks, Cybersecurity and C-TPAT, a Literature Review

Stephen Sullivan[1], Diana Garza, PhD[2]

[1]*DBA Student, University of the Incarnate Word, United States, stsulliv@student.uiwtx.edu*
[2]*Associate Professor of Business, University of the Incarnate Word, United States, dgarzaor@uiwtx.edu*

ABSTRACT: The past year has seen critical fluctuations in business operations throughout the US and the world. Due to COVID-19, employees have been encouraged or forced to work from home instead of commuting to a regular work location. Remote work has disrupted and weakened security processes. Cyber criminals have seen an opportunity in this weakened infrastructure. Cybersecurity attacks have disrupted supply chains for businesses, schools, healthcare organizations and other entities. Organizations will need to reassess security strategies with the assumption that work-from-home will become permanent. The US Department of Homeland Security has stepped up its efforts to meet this risk head-on and has incorporated supply chain cybersecurity measures within the constructs of the Customs-Trade Partnership Against Terrorism (C-TPAT) program. This all-volunteer program was launched immediately after 9/11 to thwart potential supply chain risks that could open the door to major terrorist attacks on the US homeland. This research will explore the reasons why cybersecurity has become the nation's number one commercial concern for supply chains and logistics management and how C-TPAT is enabling the proper change to the current business climate as a risk mitigating option.

KEYWORDS: cyber-security, C-TPAT, supply chain, risk

Introduction

There have been unprecedented cyber-attacks on our nation's infrastructure and, moreover the supply chain, both in the public and private sectors. Cybercriminals have been a relentless force and trend in the news headlines as many firms were subject to supply chain disruptions due to cyber-attacks on their IT systems. Supply chains are composed of a wide network of multiple businesses operating in an ever-changing and dynamic environment. Due to the interrelationships among firms, supply chains become vulnerable to a myriad of risks. Business exposure may be caused by supply chains that extend over wide geographical areas. Other possible factors for supply chain exposure include a greater demand in product customization, prices, level of service, changes in technology, a dynamic economic landscape, lifestyle changes, and natural factors (Lambert & Copper 2000).

Companies need to be proactive to survive a complex and ever-changing environment. To respond efficiently to supply chain challenges, companies must have risk mitigation capabilities and the flexibility required to respond quickly. As defined by Christopher and Holweg (2011), structural flexibility is the ability to adapt to changes in the business environment. However, efficiently responding to challenges and changes involves a higher cost in the form of additional resources.

This paper will outline the impact cyberattacks have on supply chain management including chain disruptions, risk detection, mitigation, and recovery; the magnitude of the cyberattacks and the financial and reputational losses; the role of technology and IT infrastructure, potential strategies to mitigate supply chain risks, and the overall global impact; and the role of C-TPAT in efficient supply chain management.

The intent of this paper is specific to supply chain disruptions due to cyberattacks and the role of C-TPAT to the security of such supply chains. The limitations of this study include the limited literature based on the allowed length of the paper and this paper is not an

empirical study. Further research is encouraged on this topic as it continues to involve with the integration of technology and the increased risk of cyberattacks.

Supply Chain Management

Supply chain management involves individual businesses working as a wider network. Organizations that rely heavily on supply chain management (SCM) principles do so in various ways to accomplish value-added cost reductions throughout the chain. Supply chain management (SCM) is regarded as the centralized management of the flow of goods and services which includes all programs and processes that transform raw materials into final products. The supply chain is vast and encompasses production, vendor management, demand planning, transportation (global and domestic) and logistics, purchasing, distribution, and warehousing. By managing supply chains, stakeholders and companies can cut excess costs and deliver products to the consumer faster and at a competitive price. Efficient supply chain management keeps companies out of any negative press and away from expensive recalls and lawsuits. However, in most recent studies on SCM, sustainability of the supply chain has taken center stage from both an academic and operational side.

Sustainability came to the forefront of the world's attention when the Brundtland Commission of the United Nations defined sustainable development as "development that meets the needs of the present without compromising the ability of future generations to meet their own needs" (WCED 1987). This study was a breakthrough and had a significant effect on modern SCM in terms of businesses actively seeking ways to make profits and maximize the social and economic health of the environment on which it relies. Supply chain management is on the frontline of sustainability in business as it provides a valuable opportunity for the firm to incorporate SCM objectives and performance into its decision-making processes (WCED 1987).

Sustainable supply chain management (SSCM) extends the basic concept of supply chain management by broadening performance to consider further sustainability measurements. SSCM is defined as "the management of material, information, and capital flows, as well as cooperation among companies along the supply chain, while taking goals from all three dimensions of sustainable development into account" (Meixell and Luoma 2013). Thus, SSCM involves the wider set of performance objectives identified simply as economic, environmental, and social. A firm's stakeholders can be an important factor in facilitating effective supply chain management. Stakeholders in the supply chain include any individual or group that can affect or be affected by an organization (Freeman1984). Academics look toward a stakeholder theory that suggests there should be a fit between the "values of the corporation and its managers, the expectations of stakeholders and the societal issues which will determine the ability of the firm to sell its products" (Freeman 2004). A stakeholder approach emphasizes active management of the business environment, relationships, and the promotion of shared interests which is a matter of long-term survival (Freeman and McVea 2005). However, sustainability in terms of cleaner environmental impact is paramount more now than ever.

According to the United Nations study on global transportation, the logistics aspect within the supply chain accounts for 22 percent of the world's carbon-dioxide emissions. High carbon emissions affect people, plants, animals, and the greater environment, all raising flags as to future sustainability of the world's resources and future goods and services production. Khan et. al., contend that the supply chain is intrinsically linked to the environment as the act of transporting goods globally impacts nature and that sustainable SCM depends on making better choices as far as vendors who provide low-emission options, such as compressed gas vehicles in their loading and cargo transport methods.

Supply Chain Disruptions

A supply chain disruption occurs when direct or indirect adverse and unexpected events disrupt the normal flow of the supply chain (Garvey et al. 2015). Garvey et al. (2015) differentiate between a disruption and a risk, defining disruptions as manifestations of the supply chain, whereas a risk can occur without disruption. There is also a difference between traditional and time sensitive supply chains, where time-sensitive supply chains may include disaster relief operations. DuHadway, Carnovale, and Hazen (2017), also differentiate between a disruption that is intentional and inadvertent and the source of such disruption is exogenous or endogenous. The authors further assert that intentional disruptions such as security threats are further exacerbated by weak supply chain infrastructure.

It is worth further differentiating between endogenous and exogenous disruptions. Events that occur from within the supply chain are said to be endogenous, whereas events that occur from outside the supply chain are exogenous (DuHadway et al. 2017). This research will focus on exogenous risks to the supply chain. Cybersecurity attacks or terrorist attacks are considered exogenous and impact multiple firms across various industries. Intentional exogenous disruptions lead to disruptive events for the entire network of businesses.

According to DuHadway et al. (2017), risk detection is an important component of risk mitigation strategies. Companies must be able to understand how to detect and anticipate risks to build better prevention and recovery strategies, yet not all disruptions can be anticipated. Kleindorfer and Saad (2005) posit that the robustness of the supply chain is determined by the weakest link in the entire supply chain. Particularly because of this reason, it is important to be aware of the risks that the supply chain is exposed to. DuHadway et al. (2017) assert that risk detection will be different based on the specific risk, but the detection strategies are similar in their approach. These strategies include information sharing, visibility, and integration with suppliers.

The mitigation of disruptions to the supply chain requires robust information processing capabilities. The requirements to build such capabilities must be included into a company's overall strategy. Firms with such capabilities are more competitive than rival firms. Tuggle and Gerwin (1980) suggest strategic orientations based on the information available and a response that focuses on performance. Ito and Peterson (1986) demonstrated that firm performance increases with information processing capabilities where organizations can navigate their network connections. The authors suggest that what becomes important is implementing the right capabilities and controls.

Risk recovery is based on the company's ability to recover from a disruption. Recovering from inadvertent disruptions proves to be one of the most challenging as it involves the entire network and involves the firm's ability to return to the previous state of the supply chain, also known as resilience within the literature (DuHadway et al. 2017).

Magnitude of Cyberattacks

According to IT security professionals, a cybersecurity threat is a, "malicious and deliberate attack by an individual or organization to gain unauthorized access to another individual's or organization's network to damage, disrupt, or steal IT assets, computer networks, intellectual property, or any other form of sensitive data" (Stealth Labs 2020). In today's digital world, cybersecurity measures are the key to defending a company's most precious assets. Those assets are intellectual property, customer information, financial and trade data, and employee records, among others. With increased internet connectivity comes the risk of a security breach of a company's IT systems.

A software supply chain attack occurs when a cyber threat actor, whether individual or nation-state, infiltrates a software network and introduces malicious code to compromise the supply chain software before the vendor sends it to their customers. The affected software

then compromises the customer's data or system. These attacks affect compromised software users and can have widespread consequences for government, critical infrastructure, and private sector software customers (NIST 2021). According to Industry Week (2021), and using sources from recently published IBM data, the average cost of a supply chain data breach is upwards of $3.86 million per firm or institution, not including any ransom monies that could have been paid (Industry Week 2021).

Cyber-attacks are primarily focused on the following methods: malware attacks, phishing, man-in-the-middle attack, denial of service attack, SQL code injection, ransomware attacks, and DNS attack. In terms of relative statistics, 80 percent of all cyber-attacks are through some phishing activity, and with the most prevalent, malware is the most expensive. A malware attack, costs on average $2.6 million in damages and mitigation to the average firm affected. Ransomware is said to affect the global multinational corporation sector in 2021 upwards of $20 billion in lost revenue and productivity. Additionally, a business is subject to a ransomware attack every 11 seconds in 2021, and cyber-attacks increased by 400% in the US during the coronavirus pandemic (Stealth Labs 2020).

Attacks to corporations' supply chain come from many internal and external sources. Cyberthreats are common to the following groups: nation state attacks, criminal groups, corporate espionage, hackers, malicious insiders, and terrorist groups. A leading cybersecurity watchdog organization had determined that while certain threats concentrate their efforts on acquiring ransom monies or crippling supply or manufacturing infrastructures, over 60 percent of all cyberthreats are related to malicious insider activity. According to Stealth Labs, "insider threats are perhaps one of the most concerning cybersecurity risks that IT organizations face today." Whether the threat comes from an inadvertent employee, a malicious insider, or a contractor with compromised IT credentials, these threats are virtually impossible to detect and can go unnoticed for years (Stealth Labs 2020). However, some of the most damaging cyber threats come from nation state groups.

IT Infrastructure and Cyberattacks

An area of research relative to cyber threats and infrastructure is within the strict limits of cybersecurity, or in the protection of state, local, or private hardware, software, and data from cyberattacks in internet-connected systems. The development and implementation of such technological solutions require the apportionment of scarce firm-wide IT and operations resources as well as the time to implement of management processes to shape a new organizational culture which recognizes when cyber threats are imminent. State sponsored cyber-attacks are of the most important as these threats come from well-funded and technologically savvy perpetrators. Of late, nation state attacks have been primarily focused on energy grids and their respective IT infrastructures (Stealth Labs 2020).

Recently in the US, the Colonial Pipeline was attacked by cyber criminals who shut the pipeline, causing gasoline shortages throughout the southeastern seaboard states. Joseph Blount, CEO of Colonial Pipeline Co., defended his decision to pay on the received ransom demand, $4.4 million to the culprits, noting that it was necessary to have "every tool at his disposal" to restore the 5,500-mile pipeline. The May attack on Colonial Pipeline demonstrated the security weakness of the nation's energy infrastructure and has spurred debate over how the U.S. and the oil-and-gas industry can better protect critical infrastructure against future cyber-assaults (Eaton 2021). According to a cybersecurity consultant, the attack that crippled the largest fuel pipeline in the U.S. was the result of a single compromised password. In addition to the threat brought on to the Colonial Pipeline, the attack on SolarWinds was equal in its destruction.

The SolarWinds hack was an attack primarily centered around their supply chain that compromised multiple systems of both foreign and domestic governments and companies

worldwide. This attack was initially discovered by the cybersecurity consulting firm called FireEye in December 2020. Employees at FireEye found uncommon data being sent from the company to an unknown server, which raised red flags. Regarding the formal investigation, it was discovered that one of the localized servers that provides access to software updates and data patches for SolarWinds system was compromised, thus allowing the hackers to insert malicious code into the updates and which ultimately infected multiple clients. This suspect code permitted data modification and extraction as well as allowing the perpetrators remote access to corporate IT systems that had the inserted software installed. Due to the intricacy, damage, and scope of this attack, it has since been labelled by experts as an Advanced Persistent Threat (APT) actor. Companies downstream, such as Microsoft and the US Department of Defense, were equally affected by this attack. However, it can be proposed that due to the breadth of such a high-level incident affecting multiple parties, this attack may prove the most damaging of 2020 (Downs 2020).

Cybercrime costs the global economy up to $575 billion annually. A recent survey revealed that 90 percent of organizations that rely on operational technology, including critical IT infrastructure providers, experienced a cyberattack, and over half of those organizations suffered severe downtime because of cyberattacks. Further, 37 percent of UK firms surveyed reported that malware caused significant disruptions to their operations, 33 percent admitted experiencing "significant" downtime because of a cyberattack and, and 23 percent claimed they had been hit by attacks orchestrated by nation states (Lis and Mendel 2019).

Strategies to Mitigate Disruptions

Cybercriminals are a fluid and transient group that uses hidden IT networks to attack their victims and then flee to nation-states that either support such criminals or do not have cyber crime legislation to effectively prosecute them. According to cybercrime experts, there have been instances where companies have reached out to the government, calling for increased information sharing among agencies and the private sector. Especially with the oil and gas industry, companies have insisted that the government declassify cyber events and share them throughout the industry.

The recent cyber-attacks have led to the inception of a watchdog organizations, such as the North American Electric Reliability Corp., or NERC, which controls parts of the oil and gas utilities' cybersecurity defenses and imposes fines on companies that do not meet certain IT safety standards. However, the question remains: should the U.S. government implement a similar agency or organization to ensure all American companies have cybersecurity minimum standards? The current administration (2021) has recently mandated that agencies improve their monitoring and communication efforts to detect cyberattacks and reinforce their partnerships with private industries. As a result, several cybersecurity-related bills are moving through Congress in support of these mandates. Additionally, the Transportation Security Administration, which has authority over pipeline cybersecurity, recently issued a directive that would require pipeline companies to report attacks to a cybersecurity division of the Department of Homeland Security (Eaton 2021).

Cybercrime experts state that the government has not gone far enough to combat cybercrime in the U.S. To mitigate cybercriminals' activities, the U.S. needs to strengthen its global reach to punish perpetrators who flee to countries currently out of reach of U.S. jurisdiction. Organizations have stated that the U.S. government is too slow in responding to attacks. One example of this occurred when the Ukraine power-grid was attack in 2015, the cybersecurity industry waited months for U.S. Homeland Security to give us a completed assessment. In advance of any recent governmental activities to stem any cyber-attacks, U.S. Customs and Border Protection's C-TPAT program has implemented requirements and standards for companies to take the upper hand on preventing cybercrime. A recent new

network technology called blockchain has become a new tool that can implement a forward-looking strategy to mitigate the effects of cyberattacks.

Blockchain is a type of electronic database, or more commonly referred to as an electronic ledger, which can hold critical company information. The blockchain continually grows as data are added and linked to the previous block of data using a cryptographic hash function. The result is if an attacker tries to infiltrate a blockchain network there are other chains of redundant data within the ledger stored on different computers that can provide valid backup information to complete the data chain. One advantage of the blockchain system is that for a hacker to be completely successful, one would have to affect over 50 percent of any chain node. This system is regarded as one of the best tools to avail itself over the last several years in the fight to defend systems against attack (Legrand 2020).

The Role of C-TPAT in Cyber Security Mitigation

To address cybersecurity and supply chain security measures, CBP updated the program's minimum-security requirements (MSRs) to place emphasis on acquiring mitigation relative to these supply chain risks. With special attention to cybersecurity, CBP defines cybersecurity as, "Cybersecurity is the activity or process that focuses on protecting computers, networks, programs, and data from unintended or unauthorized access, change or destruction" (C-TPAT Minimum Security Requirements 2020). It is the objective of every C-TPAT member to encourage "…the process of identifying, analyzing, assessing, and communicating a cyber-related risk and accepting, avoiding, transferring, or mitigating it to an acceptable level, considering costs and benefits taken" (C-TPAT website 2021).

With the changes made to the 2020 MSRs, CBP has given the mandate to the C-TPAT membership that cybersecurity is the next-level deterrent that mirrors the directives by the U.S. administration. CBP has introduced 10 new "must-have" and three "should-have" responses relative to cybersecurity measures that a company needs to address and demonstrate before CBP approves their application for membership. CBP goes deep into the aspects of securing IT networks and providing written guidance and instructions before the green light can be given to the member. Some evidence of CBP's requirements can be evidenced by looking at the MSRs. According to Section Four of the MSR, "Measures to secure a company's information technology (IT) and data are of paramount importance, and the listed criteria provide a foundation for an overall cybersecurity program for Members" (C-TPAT Minimum Security Requirements 2020).

Criteria included in the MSRs, focus on: providing sufficient written policy specifically related to cybersecurity defenses, a member must demonstrate and provide back-up evidencing the regular testing of IT systems to recognize IT threats, firms must install current IT security deterrent software, a system that identifies unauthorized access must be installed and reviewed on a regular basis, user access must be defined by activity and role as to defend against unwanted internal access, access to IT systems must be protected from malicious intent via the use of strong passwords, passphrases, or other forms of digital authentication, firms that have employees working remotely must secure their network by installing VPN access software, employees that access IT networks from personal computers must adhere to written cybersecurity policy governing the use of personal storage devices, etc., and finally, all media, hardware, or other IT equipment that contains sensitive information regarding the import/export process must be accounted for through regular inventories (Minimum Security Requirements 2020).

Discussion

Many high-profile cyberattacks have affected various U.S. companies over the last ten years. This research focused on supply-chain management and disruptions, infrastructure and cyberattacks,

and the role that C-TPAT has played in mitigating such attacks. This research also emphasized the limited role of government in preventing or punishing cyber criminals. It has become important that firms become more educated on cybercrime and the process of mitigation, deterrence, and prevention. Organizations and companies must do their share in defending themselves against cyber criminals. Education efforts must be part of corporate policy and operational requirements such as better password defense, phishing identification, and monitoring internal server activities. While increased corporate education surrounding cyber threats are critical paths toward defense and mitigation, the C-TPAT program offers advanced guidelines and instruction relative to the implementation of new standards for any company to use in assessing their cybersecurity program. It is the consensus of the authors that the U.S. government form a dedicated agency within the constructs of the government that has investigative, audit, and prosecution authority to address cybercrime on both the national and international levels. A suggestion, based on the present research, is to allow and give this new agency external responsibilities of transparency and information sharing through international organizations such as INTERPOL and the UN.

A newly formed agency must work seamlessly to share and disseminate information from agencies within the Departments of Homeland Security, Energy, Justice, Commerce, and State. Customs and Border Protection has taken the first step with the C-TPAT program, however, at present, the C-TPAT program only extends to companies engaged in trade and is not a mandatory nor is a statutory requirement for all U.S. companies. Many importers and C-TPAT members have argued that the requirements of the C-TPAT program must become law and that importers seeking admission to the program find the standards requisites in implementing such security guidelines. Security standards such as those outlined under the requirements for cybersecurity need to be elevated to a higher level beyond C-TPAT, Customs, or Homeland Security. New Biden Administration laws and legislation outlining cybersecurity should incorporate the requirements found in C-TPAT's MSRs and given multi-agency jurisdiction at the federal level.

References

Christopher, M., and M. Holweg. 2011. "'Supply Chain 2.0'': Managing Supply Chains in the Era of Turbulence." *International Journal of Physical Distribution & Logistics Management* 41 (1): 63- – 82. 10.1108/09600031111101439.

C-TPAT minimum security requirements for manufacturers. C-TPAT website, Customs and Border Protection, 2020. Retrieved from https://www.cbp.gov/sites/default/files/assets/documents/2019-Dec/CTPAT%20U.S.%20Importers%20MSC%202019.pdf.

C-TPAT strengthens ability to manage supply chain: *Survey U.S. customs and border protection (CBP)*. 2007.

Downs, F. 2020. "Top cyberattacks of 2020 and how to build cyberresiliency." *ISACA*, 6 November 2020, retrieved from https://www.isaca.org/resources/news-and-trends/industry-news/2020/top-cyberattacks-of-2020-and-how-to-build-cyberresiliency.

Eaton, Collin. 2021, Jul 12. "Cyberattacks and ransomware: How can we protect our energy infrastructure?" Journal report. *Dow Jones Institutional News* Retrieved from https://global.factiva.com/en/du/article.asp?accessionno=DJDN000020210712eh7c002id.

Framework for improving critical infrastructure cybersecurity. 2014. (Version 1.0. ed.). Gaithersburg, Md.: National Institute of Standards and Technology. Retrieved from http://purl.fdlp.gov/GPO/gpo46587.

Freeman, R. E. 1984. *Strategic management: A stakeholder approach*. Cambridge: Cambridge University Press. Retrieved from http://hdl.handle.net/2078/ebook:231874.

Freeman, R. E. 2004. "The Stakeholder Approach Revisited." *Zeitschrift für Wirtschafts- und Unternehmensethik 5*(3): 228. Retrieved from https://search.proquest.com/docview/225264646.

Freeman, R. E., & McVie, J. 2005. "A stakeholder approach to strategic management." *The blackwell handbook of strategic management* (pp. 183-201). Oxford, UK: Blackwell Publishing Ltd. doi:10.1111/b.9780631218616.2006.00007.x Retrieved from https://onlinelibrary.wiley.com/doi/abs/10.1111/b.9780631218616.2006.00007.x.

Garvey, M. D., Carnovale, S., & Yeniyurt, S. 2015. "An analytical framework for supply network risk propagation: A bayesian network approach." *European Journal of Operational Research,* 242(2): 618–627.

Ito, J. K., & Peterson, R. B. 1986. "Effects of task difficulty and interunit interdependence on information processing systems." *Academy of Management Journal* 29(1): 139–149.

Lambert, D. M., & M. C. Cooper. 2000. "Issues in Supply Chain Management." *Industrial Marketing Management* 29 (1): 65- – 83. 10.1016/S0019-8501(99)00113-3.

Legrand, J. 2020. "The future use cases of blockchain for cybersecurity." *Cyber Management Alliance*. Retrieved from https://www.cm-alliance.com/cybersecurity-blog/the-future-use-cases-of-blockchain-for-cybersecurity#:~:text=Blockchain%20technology%20is%20a%20distributed,record%20transactions%20between%20multiple%20computers.&text=The%20new%20technology%20is%20considered,in%20the%20integrity%20of%20transactions.

Lis, P., & Mendel, J. 2019. "Cyberattacks on critical infrastructure: An economic perspective." *Economics and Business Review 5*(2): 24-47. doi:10.18559/ebr.2019.2.2.

Llegue, O., & Richer., *CBP there's more to compliance cooperation than just C-TPAT under-utilized business-to-government relationships facilitate supply chain risk management*.

Meixell, M. J., & Luoma, P. 2015. "Stakeholder pressure in sustainable supply chain management." *International Journal of Physical Distribution & Logistics Management 45*(1/2): 69-89. doi:10.1108/IJPDLM-05-2013-0155.

Ransomware attackers used compromised password to access colonial pipeline network. (Jun 45, 2021). *CNN Wire*.

Rehman, Khan, S. A., Zhang, Y., Anees, M., Golpîra, H., Lahmar, A., & Qianli, D. 2018. "Green supply chain management, economic growth, and environment: A GMM based evidence." *Journal of Cleaner Production, 185*: 588-599. doi: 10.1016/j.jclepro.2018.02.226.

StealthLabs. 2020. "Cyber security threats and attacks: all you need to know." https://www.stealthlabs.com/blog/cyber-security-threats-all-you-need-to-know/.

Thielemann, K. Overview key findings recommendations SRM leaders in charge of technology, information and resilience risk management efforts should: Licensed for distribution.

Tuggle, F. D., & Gerwin, D. 1980. "An information processing model of organizational perception, strategy, and choice." Management Science 26(6): 575–592.

Voss, M. D., & Williams, Z. 2013. "Public-private partnerships and supply chain security: C-TPAT as an indicator of relational security." *Journal of Business Logistics, 34*(4): 320-334. doi:10.1111/jbl.12030.

World Commission on Environment and Development (WCED). 1987. *Our Common Future*. Oxford: Oxford University Press. (Frequently referred to as the Brundtland report after Gro Harlem Brundtland, Chairman of the Commission).