An Impact-Wave Analogy for Managing Cyber Risks in Supply Chains

Guerra, P.J.G.; Sepúlveda Estay, Daniel Alberto

Published in:
2018 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM)

Link to article, DOI:
10.1109/IEEM.2018.8607563

Publication date:
2019

Document Version
Peer reviewed version

An Impact-Wave Analogy for Managing Cyber Risks in Supply Chains

P. J. G. Guerra, D. A. Sepulveda Estay[1]
[1]Department of Management Engineering, Technical University of Denmark, Kgs. Lyngby, Denmark
(pabloguerra.can@gmail.com)

Abstract –**Supply chains are dependent on Information Technology (IT) and cyberspace processes. Yet, despite the advantages of its increased connectivity and systems integration with suppliers and customers, this also opens the door to new risks from and to supply chain partners. Literature in this nascent research area is limited, with few frameworks available to complement traditional risk management methods. This paper shows the current results of a literature review on the field of supply chain cyber risk management (SCCRM), with the aim of gathering and structuring its extant literature and proposing a taxonomy that will give a better overview of the approaches found in the scientific literature. This taxonomy is then used to propose a novel SCCRM framework. Finally, a novel Impact-Wave analogy is presented to provide a graphical understanding of the application of this framework.**

Keywords –**Supply Chain, Cyber Risks, Resilience, Risk Management**

I. INTRODUCTION

Modern industries face cyber-risks that are associated not only to their own data and control systems, but also to their supply chains. Organizational processes can be connected both to suppliers and customers through the internet, forming a shared network. As a result, cyber-attackers can potentially access and impact supply chains by gaining access to organizations through the weakest link in the supply network [1].

The growing complexity of supply chains, as well as an increasing sophistication in cyber-attacks, suggests that companies must prepare "for the inevitable" [2]. Consequently, it has been suggested that research focus in the area should lean more towards how to build cyber-resilient supply chains [3].

However, supply chain cyber risk management is a relatively novel field with only few frameworks available that have been specifically adapted and/or validated for the management of this kind of risks in the supply chain [3],[4].

This paper expects to contribute to closing this gap by proposing a framework derived from existing literature on supply chain cyber risks. Initially, a structured literature review reveals the approaches used to manage the risks associated to the use of information technologies (IT). Consequently, these approaches are categorized and a framework is proposed. The aim of this paper is to present the current results obtained from this process.

Section II describes the methodology that is followed. Then, section III provides a summary of the current results from the literature review. In section IV those results are analyzed to provide conceptual clarity, through the proposal and development of a framework that provides insights into how the management of cyber risks in the supply chain should be approached. Finally, section V briefly describes the future steps that result from this research.

II. METHODOLOGY

Durach *et al.* [5] propose a structured literature review (SLR) for the field of supply chain management, by following six steps: 1) defining of the research question, 2) determining of the required characteristics of primary studies, 3) retrieving baseline sample, 4) selecting the pertinent literature from the sample, 5) synthesizing the literature, and 6) reporting and using the results.

The research question is defined as "*How should the risks derived from the use of IT systems be managed along the supply chain?*". After the inclusion and exclusion criteria are determined, a baseline sample is retrieved by using different search queries that contain combinations of the keywords *supply chain*, *information technology*, *cyber*, *security*, *risk*, *management* and *resilience*. Those search queries are used in the databases Scopus and DTU Findit, obtaining a total 226 publications that meet the inclusion and exclusion criteria. Fig. 1 shows the yearly distribution of these publications from the year 2000 until February 2018.

In the fifth step, this literature is analyzed, extracting the findings and categorizing them into main themes that help on structuring the results obtained. The results shown in this study are drawn from 123 of those publications.

III. RESULTS

This section describes the current results for the two main phases of the research process: first, an overview of the supply chain cyber risk and resilience themes obtained from the SLR and second, the dynamic and event-centered approaches found in the SLR, which proposes a

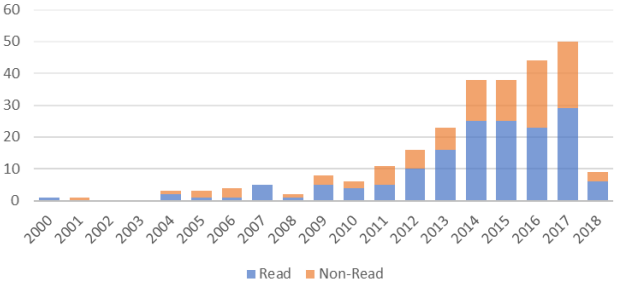

Fig. 1. Histogram of publications meeting inclusion criteria, per year.

taxonomy for these themes.

A. Research themes

The approach followed to structure the findings from the literature is the identification of themes. This process of identification and categorization results in a list of the most important knowledge areas in the field of supply chain cyber risk management, relevant answering the research question. Twelve themes are believed to gather the different approaches found in the literature towards managing those risks:

1. Compliance: In the context of supply chain cyber risk management, risk compliance can be understood as to identifying and conforming to the legislation affecting this area, as well as to the standards that must be met [4].

2. Situational Awareness: it involves the identification of potential cyber threats, vulnerabilities and risks associated to the supply chain, as well as the ability to assess the probability and impacts of occurrence of potential cyber risk events.

3. Governance: IT governance defines who, where and how decisions affecting IT are made [6]. Moreover, it can be used to provides adequate authority to cyber security to affect decisions in other managerial areas which have an impact on or are impacted by cyber risks.

4. Pre-Event Knowledge Management: it can be understood as making the best use of the knowledge available to achieve organisational objectives. Supply chain resilience can be improved by cultivating knowledge management in a situation previous to a risk-event, due to bringing a better general understanding of the supply chain and the human resources [7]. In this regard, the practices recommended are related to education and training with respect to cyber risks, and the creation of a resilience/risk management culture.

5. Cyber-Security: it refers to the protection of the assets and systems (physical or digital) involved with the storing and processing of information in digital format. Once the risks have been identified and assessed, then countermeasures must be put in place. Proactive measures and techniques used to prevent previously identified cyber risks, before the risk event takes place. In general, information security measures tend to focus on the protection of the confidentiality, integrity and availability of information [8].

6. Agility: Supply chain agility is defined as "the ability to respond rapidly to unpredictable changes in demand or supply" [9]. Two main components are identified to it, which are agility and velocity.

Visibility refers to generating knowledge and awareness on the current status of supply chain operating assets and the environment [7],[10]. It involves being able to detect risk events on the supply chain (i.e. affecting supply chain partners) which also have the potential of impacting the focal company. Finding issues as soon in the lifecycle as possible provide for time and better availability of resources to deal with them. Supply chain velocity is defined as "distance over time" [9], referring to how rapidly the supply chain reacts to disruptive events.

7. Ability to Adapt: The ability to adapt can be understood as being able to manage critical resources and operations in the supply chain and adjust them in response to challenges and opportunities [7],[10]. This ability is also covered in the supply chain resilience literature through two elements: flexibility and redundancy [7]. In this case, flexibility refers to flexibly use of processes, supply and/or demand management. Redundancy, on the other hand, builds on maintaining excess capacity as a mechanism to adapt to disruptive events [7].

8. Recovery Management: it involves the identification of critical vulnerabilities and risks that the firm should prepare for, the development of contingency plans for recovery and mission assurance after a risk event, planning for the availability of resources needed for the execution of post-disruption plans, and the effective and efficient execution of those plans when needed.

9. Market Position and Financial Strength: In the context of supply chain resilience, market position refers to the status of an organization and/or its products in specific markets, while financial strength reflects its capacity to absorb variations in cash flow [10]. Both concepts are instrumental in increasing a firm's chance of recovering from supply chain disruptions [7]. This way, market share, product differentiation and customer loyalty are some sub-factors understood to form part of the market position, while financial reserves, liquidity, portfolio diversification and insurance are elements under the broader concept of financial strength [10].

10. Post-Event Knowledge Management: Post-event knowledge management focuses on enhancing the ability of the supply chain to learn from past events, through elements like post-event feedback, improvement through education and training, and gathering of cost/benefit knowledge [7], which can be used for updating contingency plans and innovating by improving or changing resilience mechanisms [11]. Some elements proposed for pre-event knowledge management are also useful in post-event knowledge management, like education and training about information security, and the embeddedness of key learnings in the organizational security culture.

11. Social Capital: Social capital involves the network of relationships formed with suppliers, which can also be seen as a valuable asset, and an enduring source of advantage (Carey et al. 2011). Social capital contains "the information, trust and norms of reciprocity inhering within social networks" and is linked to the resilient concepts of absorbing shock and adapting to change [12], as well as a strengthened ability among the supply chain partners to learn from each other [7].

B. Dynamic and Event-centered approach

A dynamic approach is then followed to classify the findings gathered and differentiate between the different themes. A dynamic approach is one that considers time as the main variable of study.

In this case, the realization of a hypothetical cyber-related risk event is taken as our point of reference in time, and findings from the literature are clustered and presented as belonging to a moment in time that can be 1) before, 2) during or 3) after (post) the realization of this hypothetical risk event. A depiction of this perspective can be seen represented in Fig. 2.

In the literature, other authors use similar approaches, especially in the area of supply chain resilience. For example, Herrera & Janczewski [11] and Ali *et al.* [7] present frameworks where the different elements shown belong to one of the three stages in a disruption event: pre-disruption, during-disruption and post-disruption. Said division in time can also be observed through other triads of terms, like proactive, concurrent and reactive strategies; readiness, responsiveness and recovery/growth, and protection, response and adaptation [7],[11].

IV. ANALYSIS

This section describes and structures the previously identified themes into a single SCCRM framework. Then an Impact-Wave analogy is introduced and described and its application as a framework for understanding cyber-attacks is detailed.

A. Description of the framework

Taking a hypothetical risk event as a point of reference the themes are categorized as belonging to one of three different stages: pre, during and post the risk event, a seen in Fig. 2. Their position differ in relation to how far they are from the moment in time in which a risk event occurs, and whether they take place before or after said risk event.

This proposed dynamic approach positions all the identified themes in a sort of timeline, position related to to how each element interacts in time, both 1) with the prevention of, response to, and recovery from cyber risk events, as well as with their 2) short, medium or long-term effects. As a result, the main elements from section III are represented on a timeline as shown in Fig 3.

The order of the elements shown in the timeline is derived from literature, as it has been argued that Compliance can be regarded as the precedent for the management of cyber risks, where the risks and security standards to conform to exert influence into the risk assessment process [4], which forms part of Situational Awareness. Good situation awareness in the context of supply chain resilience leads to the understanding of the vulnerabilities of the supply chain and the planning for risk events, allowing for the elaboration of early warning strategies or continuity planning and the identification of supporting elements needed for them, like information sharing, coordination, and the availability of knowledge [7]. Therefore, it is understood that situation awareness is also needed early in the process of SCCRM.

Governance, on the other hand, feeds on the outcomes from compliance and situation awareness [4], defining how IT-related decisions should be made across the organization and the supply chain to manage cyber risks.

Subsequently, the previous elements define what knowledge should be created and nurtured among the members of the organization and the supply chain when it comes to managing cyber risks, which is achieved through proper Knowledge Management prior to the realization of the risk event [7].

Cyber Security mechanisms must be in place to prevent the exploitation of vulnerabilities from adversaries and to protect the goals of the supply chain from incoming threats [13]. However, if the security in place is not enough to stop the cyber-threat, then enough supply chain Visibility is needed to ensure that a cyberattack is discovered, (hopefully) before it has caused significant damage [10].

If the cyber event is spotted, then Velocity mechanisms are needed to allow for a fast response [9]. In the chaos of a disruption, the Ability to Adapt is instrumental to allow continuity of operations, through for example a flexible redistribution of resources through different processes and the use of previously redundant capacity [7].

The existence of Recovery Management programs helps in prioritizing the resources and coordinated actions needed throughout the supply chain to recover from a cyber-disruption, by providing valid contingency plans and ensuring the availability of resources needed to return the enterprise to the normal state [14]. If it turns out that there are no contingencies available, or these are inadequate, then the company will rely solely on absorbing the damage through its Market Position and Financial Strength [10].

When (and if) the mission recovers from the disruption, it is important to use the very valuable learnings gained through the experience to update and improve the practices across the different SCCRM mechanisms previously described, through proper Post-Event Knowledge Management [7]. Finally, the Social Capital that is formed in turbulent times is also a valuable asset,

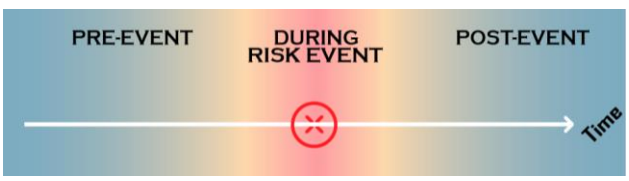

Fig. 3. A dynamic view of risk events.

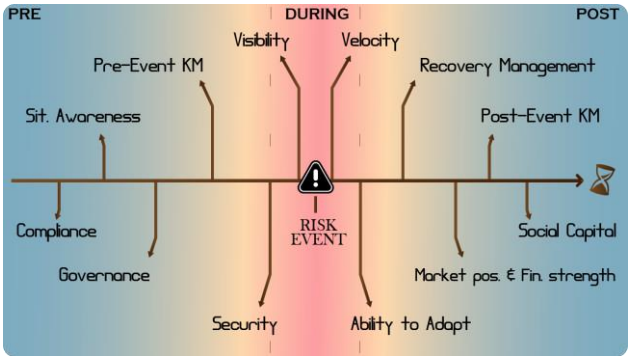

Fig. 2. The proposed SCCRM Framework.

that can enhance collaborative attitudes across different levels in the supply chain, towards a better management of the common risks faced and the exploitation of new opportunities [12].

This sense of distance in time allows for alternate approaches to the problem of managing cyber risks in the supply chain, through the introduction of concepts like strategic and tactical elements, as depicted in Fig. 4.

If we understand strategic elements as those that look at the problem from a more long-term point of view, and tactical mechanisms as those that approach it from a shorter time span, then this division allows to identify mechanisms that are more relevant in either the short (tactical) or the long (strategical) term, before and/or after the realization of a risk event, and how they can complement each other in carrying out a holistic approach towards SCCRM.

B. Impact-wave analogy

The themes that were found in literature and places in the timeline can be better understood through the use of an analogy, which considers the ripple or wave created by an impact against a surface (e.g. like ripples on the water).

As part of this analogy, the timeline represents the perspective of a focal organization, which forms part of a supply chain. The point of reference is the "point of impact" in which a cyber-event "hits" the organization, as in Fig. 5.

From the point of view of time, for a risk to successfully impact the organization, it must cut across a number of defensive mechanisms on the left side, located either far in time (strategic mechanisms) or close (tactic/operational mechanisms). These can also be understood as lines of defense.

When the lines of defense are not able to stop a cyber-event, an impact takes place. This impact then creates a "shock wave", or a "ripple", that can expand in time as shown in Fig. 6. The magnitude of those waves and their reach will depend on a number of factors. On the left side of the framework, there are the elements that can reduce the strength of (or even stop) the impact (i.e., in this analogy the speed at which the cyber-bullet impacts the system), which will directly affect the magnitude of the shock wave on impact. However, the function of the elements placed on the right side of the framework is to

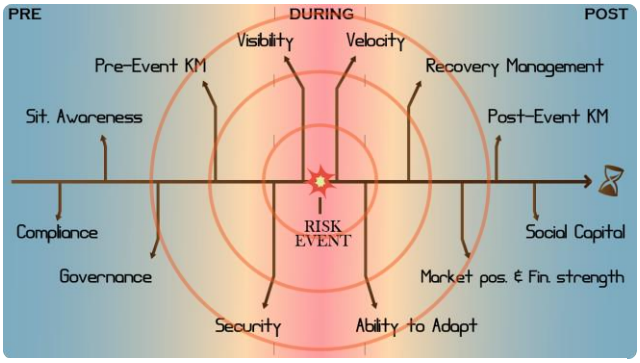

Fig. 4. The impact of a successful cyber-attack can be "felt" over time.

mitigate the "disastrous" effects of those waves by absorbing them. For the sake of this analogy, it can be understood that these waves are able to reach as far as the next absorption mechanism in place is able to absorb a shock wave of equal or bigger magnitude. If a wave is stronger than what a certain mechanism can absorb, then its effects will continue to spread and the next mechanism in time will have to actuate, until the shock wave is stopped.

On the left side, it could be that the regulatory requirements are not enough to adequately address a certain cyber-threat. If this threat is not made aware of as part of the risk identification and assessment process, then different governing processes and structures may not be in place to correctly address them, and the knowledge management (KM) needed to treat it will not be there either. It could also happen that this cyber-attacker, making use of an inherent vulnerability in the system, is able to avoid the cyber security in place. Then, if the Visibility mechanisms are not designed to detect the actions of a cyber-attack whose possibility has not been identified before, the organization might have been hit by a cyber-event without (maybe) being able to notice it.

For example, if a cyber-breach occurs and the Visibility and Velocity mechanisms in place are not able to detect and react to the attack fast enough, then Adaptive mechanisms could also be not enough to contain and stop it from spreading and/or allowing the attackers to take a foothold into the IT systems of the organization. If such a breach escalates, then the organization starts relying on the existence of contingency plans to recover from the disruption, together with facing a test on its financial and market strength.

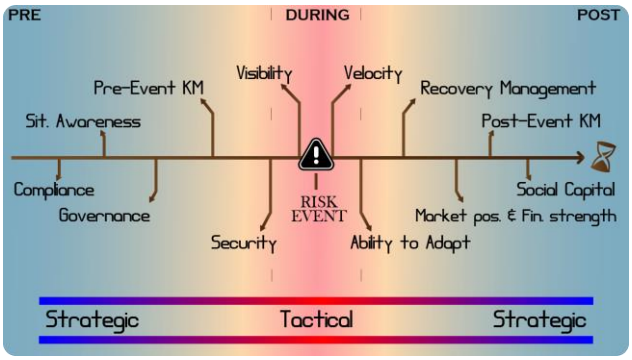

Fig. 5. Strategic vs Tactical SCCRM themes.

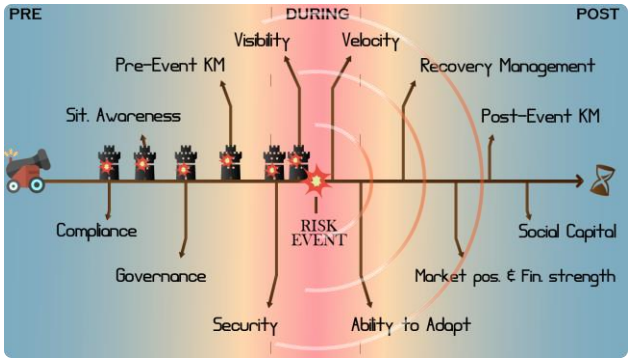

Fig. 6. Analogy of the Impact-Wave of a successful cyber-attack.

If an organization is not able to stop this "wave", then the "disaster" could become comparable to that of a "cyber-tsunami", in which the continuity of the company's mission is at stake. Maybe the effects of a cyber-tsunami (Fig. 7) are not the same as a real one but, even though an organization's physical assets might still be there for some more time, their business model could have been left ineffective, due to financial unsustainability as a consequence of, for example, loss of competitive advantage (from IP theft), reputation, increased costs or technical impossibility of continuing critical operations within a reasonable timeframe.

At this point, the only things left for the organization might be their social capital (like the personal and collective knowledge contained in the organization, and the value of the network of personal relations formed within the value chain), and learning from past experiences, which could be used to innovate and build a new start for the organization, if so.

V. CONCLUSIONS AND FUTURE WORK

Nowadays, IT systems and cyberspace have an ever-greater presence in industries and their supply chains, through modern concepts like the Industry 4.0, the Internet of Things and Cloud services. This, however, also opens the door to vulnerabilities from and to supply chain partners. Nonetheless, there seem to be few frameworks in the literature that specifically approach the management of supply chain cyber risks.

To shed light into how to manage this specific kind of risks, a literature review on the field of supply chain cyber risk management (SCCRM) is conducted, gathering a significant amount of knowledge applied in this area. Then this knowledge is structured into different themes, providing a taxonomy that gives a better overview of the different approaches proposed in the scientific literature. Those constructs are then linked through the proposition of a SCCRM framework, where all the previously identified themes can be analyzed from a time-dynamic perspective, and a novel Impact-Wave analogy is proposed to provide conceptual clarity.

Future work on this area would include a complete analysis of the scattered SCCRM literature, to ensure full coverage of the themes present in the literature. The external validation of the framework must be explored through the development of case studies to, on one hand, evaluate the suitability of this framework for analyzing past supply chain cyber events, while on the other it should be explored how it can be practically implemented to better manage supply chain cyber risks.

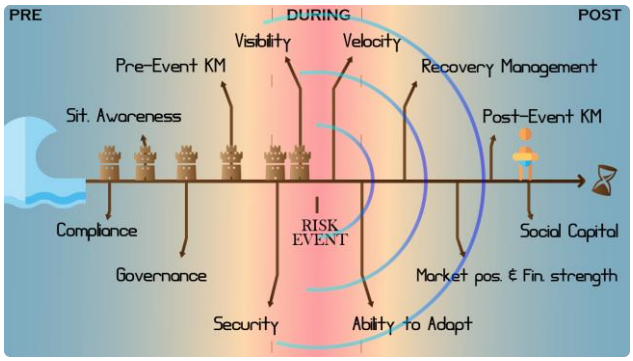

Fig. 7. The analogy of a cyber-tsunami.

REFERENCES

[1] H. He et al., "The security challenges in the IoT enabled cyber-physical systems and opportunities for evolutionary computing & other computational intelligence," 2016 IEEE Congress on Evolutionary Computation (CEC), Vancouver, BC, 2016, pp. 1015-1021.

[2] PwC, "Strengthening digital society against cyber shocks", in Key findings from The Global State of from The Global State of Information Security® Survey 2018, PwC, London, UK, 2017. Available: https://www.pwc.com/us/en/cybersecurity/assets/pwc-2018-gsiss-strengthening-digital-society-against-cyber-shocks.pdf [Accessed June 1, 2018].

[3] O. Khan and D. A. S. Estay, "Supply Chain Cyber-Resilience: Creating an Agenda for Future Research," Technol. Innov. Manag. Rev., no. April, pp. 6–12, 2015.

[4] B. Gaudenzi and G. Siciliano, "Managing IT and Cyber Risks in Supply Chains," in Supply Chain Risk Management: Advanced Tools, Models, and Developments, Singapore: Springer Singapore, 2018, pp. 85–96.

[5] C. F. Durach, J. Kembro, and A. Wieland, "A New Paradigm for Systematic Literature Reviews in Supply Chain Management," J. Supply Chain Manag., vol. 53, no. 4, pp. 67–85, 2017.

[6] R. Patnayakuni and N. Patnayakuni, "Information Security in Value Chains : A Governance Perspective," Twent. Am. Conf. Inf. Syst., pp. 1–10, 2014.

[7] A. Ali, A. Mahfouz, and A. Arisha, "Analysing supply chain resilience: integrating the constructs in a concept mapping framework via a systematic literature review," Supply Chain Manag. An Int. J., vol. 22, no. 1, pp. 16–39, 2017.

[8] H. Boyes, "Cybersecurity and Cyber-Resilient Supply Chains," Technol. Innov. Manag. Rev., vol. 5, no. 4, pp. 28–34, 2015

[9] M. Christopher and H. Peck, "Building the resilient supply chain," Int. J. Logist. Manag., vol. 15, no. 2, pp. 1–13, 2004.

[10] T. J. Pettit, K. L. Croxton, and J. Fiksel, "Ensuring supply chain resilience: Development and implementation of an assessment tool," J. Bus. Logist., vol. 34, no. 1, pp. 46–76, 2013.

[11] A. Herrera and L. Janczewski, "Cloud Supply Chain Resilience: A Coordination Approach," 2015 Inf. Secur. South Africa, pp. 1–9, 2015.

[12] N. Johnson, D. Elliott, and P. Drake, "Exploring the role of social capital in facilitating supply chain resilience," Supply Chain Manag. An Int. J., vol. 18, no. 3, pp. 324–336, 2013.

[13] H. Goldman, R. McQuaid, and J. Picciotto, "Cyber resilience for mission assurance," 2011 IEEE Int. Conf. Technol. Homel. Secur. HST 2011, pp. 236–241, 2011.

[14] S. A. Torabi, R. Giahi, and N. Sahebjamnia, "An enhanced risk assessment framework for business continuity management systems," Saf. Sci., vol. 89, pp. 201–218, 2016.