2016 European Intelligence and Security Informatics Conference

A Quantitative Approach to Risk and Cost Assessment in Supply Chain Management

Linus Gisslén and Andreas Horndahl
Swedish Defence Research Agency (FOI)
Stockholm, Sweden
{linus.gisslen, andreas.horndahl}@foi.se

Abstract— **Risk management for large and complex networks (e.g. supply chains) is difficult since there are often numerous vulnerabilities and the impact of a disruption is hard to predict. The strive for increased effectiveness often increases complexity and vulnerability rendering it even harder to foresee disruptions and their effects. Methods and tools that can be used for reasoning about risks and counter-measures are therefore needed. This paper introduces a method to assess identified risks together with available de-risking and mitigation strategies to calculate the disruptions expected effect on the network flow. Risks are expressed as functions of probabilities and impacts allowing for quantification of the disruption cost building on formalized relations. The contribution of this paper is a method which assists with estimating the total expected cost of disruptions including the counter-effect of mitigation strategies, consequently allowing for a balanced efficiency vs. disruption resilience plan. The method is suited for implementing in a decision support tool enabling cost-benefit analysis for a large number of risks and mitigation strategies.**

Keywords—supply chain risk, mitigation strategy, de-risking, strategy assessment, risk management

I. INTRODUCTION

Any complex network such as a supply chain or a computer network is inevitable exposed to the risk of partial or complete failure. Disruptions needs to be controlled as it negatively affects the flow and consequently the output. As redundancy decreases and the complexity of supply chains (SCs) are increasing [1], so does their vulnerability to a negative event [2]. As a consequence of increased optimization supply chains are nowadays more efficient during normal times, but cost and frequency of disruptions are steadily increasing. This effect, combined with globalization and heavily reliance on global transportation, significantly magnifies negative effects of disruptions. A supply chain failure means a cost of some type and magnitude and can be expressed both as a direct financial cost but often in a more indirect way expressed as time delay, customer loss, injuries, negative goodwill, etc. It is not always straightforward how to valuate these different costs against each other.

There are many domains which deals with management of risk and subsequent costs. Risks does not always mean the same thing even though the approach to reduce it could be similar. For example in supply chain management, risk can be defined as the disruption of information, materials, products and money flow [3], in computer network risks are e.g. down time, consumer experience, and security, and in humanitarian demining risks are e.g. causalities, injuries and monetary costs [4].

A strategy can be anything from a single simple counter-measure up to a highly complex strategic plan involving many steps and measures. In this paper we will use the word *strategy* to cover this whole spectra. Comparing different strategies to reduce the cost of disruptions in the supply chains is not trivial, especially when the number of risks and strategies are in the hundreds. For each failure point there might be numerous factors and each failure might have indirect and cascading effects making it hard to foresee all consequences. Also each strategy might come with a cost which is not negligible and has to be considered when a strategy is evaluated and compared to other strategies. The cost might even render many of these strategies inefficient as they cost more to implement than they save. The motivation for this paper is this identified shortcoming on how to quantitatively compare, combine and rank different strategies. Therefore, to assist the analysis of de-risking and mitigation strategies we propose a method to quantify the effect of different strategies. This enables implementation of decision support tools to compare different strategies with the aid of quantified values. In this paper we will present the outline of the method.

II. RELATED WORK

Any complex network has a large source of potential risks which can lead to disruption, and there is unavoidably a tradeoff between efficiency and vulnerability to disruption [5]. Several approaches to risk assessment frameworks which identifies risks has been developed recently resulting in several approaches to categorize risks. Mitroff et al. divides risk into different categories: natural accidents, normal accidents and abnormal accidents [6]. Kleindorfer et al. divides risk into operational risk (e.g. equipment failing, human errors, etc.) and disruption risk from normal activities (e.g. natural hazards, terrorism and political risks) [7]. Gaonkar et al. divides the risk management problems into three levels: strategic, operational and tactical. They argue that it leads to a more robust supply chain design [8]. A comprehensive guide to identify vulnerabilities in supply chains can be found in [5].

Choi et al. has identified that the reason why disruptions are more common now is due to the search for efficiency and cost-reduction during the normal state [1]. Hence, in the realm of supply chain the critical risks are the disruption of flows of information, material products and money between organizations. How the consequence of a disruption can be

978-1-5090-2857-3/16 $31.00 © 2016 IEEE
DOI 10.1109/EISIC.2016.54

IEEE computer society

mitigated is discussed in [9] where also disruption discovery and recovery is examined.

The process to develop risk mitigation strategies varies. Kleindorfer et al. suggests a step by step process which assesses the critical vulnerabilities of the supply chain [7]. Christopher et al. suggests that improving the information that the supply chain managers receives helps with mitigating the risk [2]. This is an abstract strategy trying to improve confidence in the supply chain. Chopra et al. is using a framework for identifying potential risks to the SC [10]. Chopra suggests multiple specific risk mitigation strategies analyzing the risk probability and the cost of implementing the strategy. The method presented in this paper is probably closest to supporting Chopras et al. framework.

III. METHOD

Herein we propose a method to quantify the direct and indirect costs of disruptions in e.g. supply chain, computer network, hospital emergency, etc. In order to correctly account for cost we suggest a formal method of calculating the effect of de-risking and mitigation strategies. The disruption types and network design combined will decide the baseline disruption cost which may be mitigated by selected strategies. These factors (disruptions, network and strategies) decides the final cost. This method focus on how to analyze the *combined effect* of these factors and not on how to analyze these factors individually (see Sect. *II* for excellent guides on this).

A. *Impact and cost*

Often in the domain of supply chain an aggregated qualitative measure of all the costs involved is conveyed as an impact measure expressed qualitatively as e.g. *Low Impact*, *Moderate Impact*, etc. [11]. However, cost can also be expressed as a quantitative measure of impact expressed in numerical values. Individual components of impact can be expressed as tangible assets such as money, time (e.g. lead time), lives, injuries, etc. but also intangible assets such as goodwill, reputation, competitive positioning, etc. Tangible assets are usually easier to express numerically while intangible assets are depending on an analyst comprehension and experience to be quantized. Furthermore, describing cost in a quantitative fashion allows for a more formal comparison between different strategies. In this paper the aim is to leverage the qualitative analysis by taking advantage of the quantitative expression of cost. Therefore in the following focus is on the quantitative measure of cost as qualitative approaches has been thoroughly discussed elsewhere, e.g. [11].

B. *Likelihood and probability*

Similarly in the domain of supply chain the likelihood of an (disruption) event is often expressed as a qualitative value, e.g. Likely, Unlikely, Neutral, etc. [11]. This representation is not particularly well suited when calculating absolute values. Fortunately the probability can instead be expressed in quantitatively numerical values estimated from either similar situations and conditions, or deduced from historical data, to allow for numerical calculations. Therefore, similar to the impact parameter (see IIIA) to allow for a quantitative estimation of an event the probability value is required. Consequently in this paper we will only use the absolute probability measure.

To estimate the probability of an event e mainly two approaches can be used. The first is the most obvious and straightforward: the analyst approximates the P_e (probability of event e to occur) by looking at historical data, experience, or by other method estimating a probability for a given event. The second approach is to aggregate all the underlying possible incidents that lead to the event into an estimation of a probability value (compare Fig. 1). Formally this can be written as $P_e = 1 - \prod_{n=1}^{N}(1 - P_i^n P_{ei}^n)$, where P_i^n is a prior incident probability, P_{ei}^n is the probability that once incident i occurs it causes event e, and N is the number of possible prior incidents. $P_i^n P_{ei}^n$ should be interpreted as: the probability of the incident i to occur and cause event e. Here setting $P_{ei}^n = 1$ assumes that an incident will certainly result in the event e to occur.

Even though the second approach is more tedious to approximate P_e, this approach can be advantageous as it allows us to include prior knowledge. For example, prior knowledge can come from:

- Changed conditions: For example an earthquake prone area might indirectly increase the probability of road blocks and bridge failure on a cargo route which consequently affect the P_e value. Here the second approach can include the knowledge about the earthquake frequency allowing for recalculating the probability P_e.
- New facts: When a verified fact is reported, by setting $P_i^k = 1$ we can instantaneously incorporate this new piece of information into the calculation of P_e. For example, if a road block is observed/reported the final $P_e$can be better estimated by including this piece of information.
- Intelligence: When estimating the probability of e.g. a cyber-attack several factors is considered such as opportunity, ability and intent. If intelligence says that any of these factors increases also the probability of an (successive) attack increases. In Fig. 1 it is illustrated how different incidents may affect the probability of an event.

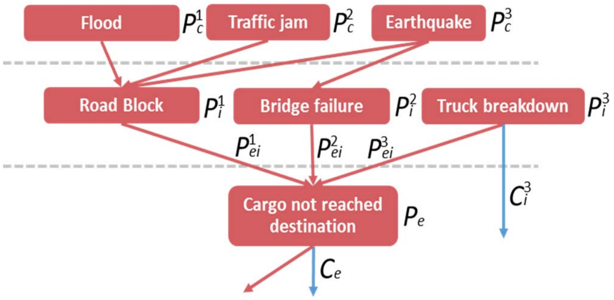

Figure 1: An illustration of different factors affecting the probability of an (risk) event. Here the event is represented by "Cargo not reached destination". The event probability $\boldsymbol{P_e}$ *is a function of all possible contributing factors and their probabilities* $\boldsymbol{P_i^n}$ *and the probability* $\boldsymbol{P_{ei}^n}$ *it will cause the event. The contributors can in their turn be dependent on other causes (such as "Earthquake" here). The red arrows represents a probability contribution (denoted* **P***) and the blue represents a cost contribution (denoted* **C***) for the organization.*

The occurrence of an event can lead to two things. Firstly, a cost may be associated with it which can be used in the risk exposure calculation. Secondly it may be causing other events which in turn may have further cost associated to it and thus having an indirect cost to the network. This is illustrated by the *Truck breakdown* incident in Fig. 1. It has both an intrinsic cost (repair) and an effect of the probability of the cargo to reach its destination (assuming the truck is carrying cargo). Consequently in turn, the *Cargo no reached destination event* can have indirect effects even further down the supply chain.

C. Risk exposure and expected cost

Now that we have a way of expressing both cost and probability quantitatively we examine the expected cost variable, often referred to as *exposure* in the domain of supply chain. A straightforward way to evaluate and estimate risk exposure is to use the relation *exposure = likelihood · impact* [12]. This can be translated into a relative number which can be used to compare and rank risks. However, as previously mentioned to get a quantitative and absolute measure of exposure the *probability* and a quantitative measure of *cost* of an event is needed [13]. Therefore, following previous reasoning we assume that the *likelihood* value can be expressed as a *probability and* the *exposure* can be expressed as the *expected cost* (***E****c*). If *y* is an event the expected cost of this event can then be written as:

$$\boldsymbol{E}_c\,(y) = P_e\,(y)\cdot \boldsymbol{C}_f\,(y). \tag{1}$$

Where $P_e(y)$ is the probability of an event *y* and $\boldsymbol{C_e}(y)$ is the aggregated cost containing different cost types:

$$\boldsymbol{C}_e(y) = \sum_{k=0}^{N} \alpha^k C_e^k(y). \tag{2}$$

The equations expresses the relation that the aggregated cost is the sum of all possible cost types. Here $C_e^k(y)$ can be money, lead time, goodwill, human injuries/causalities, etc. as discussed earlier. α^k is the weighted importance of each composite so that each component can be attributed their relative impact. The weighted value α^k can also be used to fuse the components to a single value to allow for a ranking between different strategies. It is done by setting the inversed unit as the individual weight, e.g. if $C_e^n(y) = 1\$$ then setting $\alpha^n = \$^{-1}$ will make it a unit-less value. Now that expected cost can be expressed in a formal way it is possible to study how different cost reduction strategies affects the final cost.

D. De-risking and mitigation

There are mainly two ways to reduce the negative impact (i.e. cost) of an event. Either reduce the *probability* of the event of occurring (de-risk strategy), or reduce the *impact* it has when it actually do occur (mitigation strategy). For a mitigation strategy (e.g. insurances) the mitigated expected cost $\boldsymbol{E}_c^*(y)$ for event *y* can be written as:

$$\boldsymbol{E}_c^*(y) = P_e(y) \cdot min\{\boldsymbol{C}_e^*(y), \boldsymbol{C}_e(y)\} + \boldsymbol{C}_m. \tag{3}$$

Where $\boldsymbol{C}_e^*(y)$ is the mitigated cost of the event including other costs such as deductible, increased risk premium, etc. The *min* condition says that if the cost of $\boldsymbol{C}_e^*(y)$ is larger than $\boldsymbol{C}_e(y)$ (e.g. deductible is larger than the cost) then the cost falls back to $\boldsymbol{C_e(y)}$. ***C****m* is the implementation cost of the mitigation strategy.

Here we separate mitigation strategy cost ($\boldsymbol{C}_m$) from de-risking cost as they affect different parameters. To include the de-risking strategies, where the probability $P_e(y)$ is reduced, the equation is extended to

$$\boldsymbol{E}_c^*(y) = P_e^*(y) \cdot min\{\boldsymbol{C}_e^*(y), \boldsymbol{C}_e(y)\} + \boldsymbol{C}_m + \boldsymbol{C}_d. \tag{4}$$

Here P_e^* is the reduced probability and ***C****d* is the implementation cost of the de-risk strategy. This is a formal way of expressing the different contributing cost. A de-risk and mitigation strategy may of course have an effect on several events so the cost might be divided between those strategies. For example, a network firewall (de-risk strategy) might decrease the probability of both a "Server crash" event and a "Stolen passwords" event. These above equation is similar to Shavell's model on the occurrence of accidents and liability [13] where level of care corresponds to the mitigating cost (C_m).

With this it is possible to quantify and compare different strategies as long as their respective parameters are known or can be adequately estimated. It makes it possible to pinpoint under which condition each strategy becomes profitable and how combining different strategies affects the final expected cost. Any number of cost types and strategies can be compared with this method.

E. Numerical example

To illustrate how the method can be applied we use a simple but illustrative example in the field of SC conserning shipments. Here the baseline average cost (top line Fig. 2) of disruption consists of two components: one in money (measured in \$) and one in lead time delay (measured in hours). We compare applying two different strategies (one mitigation strategy costing \$8k and one de-risking costing \$6k) one at a time, and then applying both strategies simultaneously. In this example the mitigation strategy reduces the cost of disruption to half and the de-risking strategy halves the risk of disruption. Here we set $\alpha^1 = \alpha^2 = 1$ (weighting parameters from Eq. 2) so that the units are kept and the different cost types are separated. In this example the calculated cost is the smallest for the risk-reduction

Baseline cost:

$$C_e = \$100k + 5h, P_e = \frac{0.2}{trip} \Rightarrow \qquad E_c = \frac{\$20k+1h}{trip}$$

Sole mitigation strategy:

$$C_e = \$50k + 5h, C_m = \frac{\$8k}{trip}, P_e = \frac{0.2}{trip} \Rightarrow \qquad E_c = \frac{\$18k+1h}{trip}$$

Sole risk reduction strategy:

$$C_e = \$100k + 5h, C_d = \frac{\$6k}{trip}, P_e = \frac{0.1}{trip} \Rightarrow \qquad E_c = \frac{\boldsymbol{\$16k+0.5h}}{\boldsymbol{trip}}$$

Mitigation + Risk reduction strategy:

$$C_e = \$50k + 5h, C_{m+d} = \frac{\$6k+\$8k}{trip}, P_e = \frac{0.1}{trip} \Rightarrow E_c = \frac{\$19k+0.5h}{trip}$$

Figure 2: Example of shipment cost expressed in both money and delay. Here the sole risk reduction strategy is the most cost effective.

strategy and therefore the preferable one. This example is a simple illustration of how cost can be decomposed and treated as separate units (to merge the values and obtain an relative ranking we can e.g. set $\alpha^1 = \frac{1}{\$}, \alpha^2 = \frac{1}{h}$).. As previously mentioned any cost unit can be added (money, lead time, down time, goodwill, injuries/causalities, etc.).

IV. APPLICATION AND CONCLUSION

A. Application on different strategies types

In the following we will discuss how this method can be used by different high-level standard strategies.

1) Supply management strategies

- Multi-supplier strategy. Here the cost is in term of e.g. money and reduced quality control. Supplier can be factories or web services providers and there is a direct cost of keeping this redundancy.
- Real options strategy is a way of keeping a backup supply to ensure that even if a disruption happens, there is another supplier ready to deliver supply.

These strategies should be straightforward to quantify into different decomposed costs so they would certainly be possible to analyse with the proposed method.

2) Product management strategies

Product management strategies are similar to supply management strategies as they involve a kind of redundancy allowing for the production or transport to go on independently if part of the SC fails. Similarly, it is then possible to estimate the probabilities and the cost of these kind of strategies which should make the method presented here suitable.

3) Demand management strategies

- Responsive pricing strategy is using price as a measure to control demand.
- Demand postponement strategy which is trading time delays with revenue by for example offering discount to the customer for a late shipping.

These strategies is harder to evaluate with the method presented in this paper as it is an active strategy requiring interaction with customers. Disruption is harder to predict quantitively, as well as cost for each strategy as it depends on so many factors.

4) Information management strategies

- Information sharing strategy improves the communication and efficiency within the network. Having accurate and timely information reduces the risk of forecast errors and increases the time to react to a decrease of demand.
- Resilience information system strategy is aiming to make the information system more resilient by redundancy.

Failure in the information management system is often a very critical disruption. The cost of de-risking and mitigation can however often be estimated as the strategies are fairly straightforward with investment in e.g. material and personnel.

All of the above mentioned strategies are generally high-level strategies. This method can be used to quantify high level strategy if all the individual measures can be decomposed and evaluated. Individual measures (e.g. rerouting, insurances, increasing stock, increasing suppliers, investments, etc.) can similarly be analyzed following the same reasoning as above.

B. Conclusion

There is always a trade-off between costs of cost reduction strategies and the disruption cost itself. Some strategies are just too costly to be useful, and some disruptions are too rare be worth building a de-risking strategy around. Combining different strategies might not give the synergy effects intended and might even cancel each other out. It can be difficult comparing different strategies and how they work together especially if there are hundreds of them. As highly complex strategies which applies multiple risk mitigation approaches quickly tends to be too complex to evaluate by hand. The concept described here is a way to formalize the evaluation of mitigation and de-risking strategies so that it can easily be implemented in a decision support tool. The method described is intended to be general enough to be applied to various risk management areas such as supply chains, terrorism risk, humanitarian demining, cyber security, etc. In this paper we have argued that the method presented can improve the analytical power of an analyst within the field of risk management.

ACKNOWLEDGMENT

This work was partially supported by the European Union's FP7 research and innovation programme under grant agreement No 603993. The authors would like to thank Farshad Moradi for valuable discussions and comments.

REFERENCES

[1] Choi, T. Y., and Krause D. "The supply base and its complexity: Implications for transaction costs, risks, responsiveness, and innovation." Journal of Operations Management 24, no. 5, 2006, pp. 637-652.

[2] Christopher, M., and Lee H. "Mitigating supply chain risk through improved confidence." International journal of physical distribution & logistics management 34, no. 5, 2004, pp. 388-396.

[3] Jüttner, U. "Supply chain risk management: Understanding the business requirements from a practitioner perspective." The International Journal of Logistics Management 16, no. 1, 2005, pp. 120-141.

[4] Gisslen, L., and Torne A. "A Semantic Approach to Information Management and Decision Support: An Application to Humanitarian Demining Operations." EISIC, 2015, pp. 75-82. IEEE.

[5] Stecke, K. E., and Kumar S. "Sources of supply chain disruptions, factors that breed vulnerability, and mitigating strategies." Journal of Marketing Channels 16, no. 3, 2009, pp. 193-226.

[6] Mitroff, I. I., and Alpaslan, M. C.. Preparing for evil. Harvard Business School Pub., 2003.

[7] Kleindorfer, P., and Saad G. "Managing disruption risks in supply chains." Production and operations management 14, 1, 2005, pp. 53-68.

[8] Gaonkar, R., and Viswanadham N.. "A conceptual and analytical framework for the management of risk in supply chains." IEEE International Conference on, vol. 3, 2004, pp. 2699-2704.

[9] Blackhurst, J., Craighead, C., Elkins, D., and Handfield, R. "An empirically derived agenda of critical research issues for managing supply-chain disruptions." IJPR 43, no. 19, 2005, pp. 4067-4081.

[10] Chopra, S., and Sodhi. M. S. "Managing risk to avoid supply-chain breakdown." MIT Sloan management review 46, no. 1, 2004, pp. 53.

[11] Oke, A., and Gopalakrishnan M. "Managing disruptions in supply chains: a case study of a retail supply chain." IJPE 118, no. 1, 2009, pp. 168-174.

[12] Aven, T, and Renn O. "On risk defined as an event where the outcome is uncertain." Journal of risk research 12, no. 1, 2009, pp. 1-11.

[13] Shavell, S. "A model of the optimal use of liability and safety regulation." The RAND Journal of Economics 15, no. 2 , 1984, pp. 271-28