Supply chain risk categories

Introduction

There have been many different definitions of supply chain risk, but it can be broadly defined as “ the variation in the distribution of possible supply chain outcomes, their likelihood, and their subjective values” (March & Shapira, 1987, p. 1404). However, this definition has since been expanded upon to account for all the different departments and functions that operate within a supply chain. This leads to an overall definition of supply chain risk as “ any risks for the information, material and product flows from original supplier to the delivery of the final product for the end user” (Juttner, et al., 2003, p. 202). Simply put, supply chain risk refers to the probability of a risk event occurring the supply line and when the product goes on sale. Furthermore, risk sources are the predominant causes of risk events, which are “ the environmental, organisational or supply-chain variables which cannot be predicted with certainty and which impact on the supply chain outcome variables” (Juttner, et al., 2003).

Identifying Supply Chain Risk

There are a variety different approaches that a company can take in order to identify risk in their supply chain. Steele and Court (1996) proposed a conceptual framework for identifying the potential risk in an organisations supply chain. This process was comprised of three key steps:

1. The probability of a risk event occurring in an organisations supply chain must be determined.

2. Next, the organisation should attempt to estimate the likely duration the risk event will last for, including when it may occur. This can usually be achieved through the analysis of past experiences.
3. Lastly, an analysis should be conducted on the probable impact the risk event could have on a certain facet of the organisation, such as market or financial performance.

If a company goes through these stages every time they believe a risk event may be imminent, then it will allow them to successfully identify the severity of the risk event, and put in motion any plans to prevent the risk.

Furthermore, an organisation should constantly be monitoring and attempting to identify risk events, as the earlier a risk is identified, the more likely it will be that an organisation that limit or completely negate the effects. If a company is conducting a new project to improve the supply chain, then risk identification should occur during the planning and preparation stage. This means that the organisation will have to identify risk indices, which aim to give a quantitative analysis of the potential risks associated with a project (Turney, 1996).

After the risk has been successfully identified, it can be categorised into a variety of different supply chain risk categories. This report will aim at identifying three supply chain risk categories, and suggest ways in which risk can be mitigated or managed within these categories. The three supply chain risk categories that will be explore are; exogenous, data integrity and internal resource risks.

Exogenous or External Threat

The supply chain must deal with external forces, such as natural disasters (flooding, hurricanes, or earthquakes) or human-centred issues (fraud or terrorism). Gupta & Maranas (2003) classify exogenous risk into two main sections. The first is long-term uncertainties, which can be in the form of seasonal demand variations or raw material unit price fluctuations. On the other hand, risk could cause short-term uncertainties, such as cancelled/rushed orders or equipment failure.

There are a plethora of issues present when trying to manage exogenous risk. This is mainly in the form of company's unwillingness to plan for large-scale disruptions. Although organisations generally aim to protect themselves from small, recurrent exogenous risks, they ignore the high-impact, low probability ones (Chopra & Sodhi, 2004; Faisal, et al., 2006).

One of the most prominent strategies for mitigating the impact of exogenous risk events, is through the use of ' hedging'. Hedging is a " supply side risk management strategy. In a global supply-chain context, hedging is undertaken by having a globally dispersed portfolio of suppliers and facilities such that a single event" (Manuj & Mentzer, 2008, p. 208). This is a particularly strong strategy at mitigating exogenous risk, especially high-impact ones, because it reduces the amount of operations that a potential natural disaster will hit. Furthermore, there are a variety of ways in which an organisation can ' hedge' against exogenous risk. One of the most prominent ways is through the use of dual sourcing, which protects the quality, quantity, price and performance of products by sourcing from more than one supplier. Furthermore, these suppliers must be far enough apart to ensure

that a natural disaster wouldn’t affect both of them. Although a strong strategy, it is incredibly expensive for a company to do, as dual-sourcing is much more costly then single-sourcing (Berger, et al., 2004). Hedging is the best technique to use if a company has the available investment resources, faces high levels of exogenous risk, and produces goods where strong quality and process controls are in place.

Furthermore, an organisation can use the Supply Chain Operations Reference (SCOR) framework. This model comprised of four factors; source, make, deliver and plan. The SCOR framework can be used to “ improve alignment between marketplace and the strategic response of a supply chain, on the premise that the better the alignment, the better the bottom line performance” (Huan, et al., 2004, pp. 24-25). Although it doesn’t identity risks, it acts as model to increase the performance of the supply chain and make it more resilient against potential risk events. A resilient supply chain has the ability to return to its original or desired state after being disturbed by a risk event (Peck, et al., 2003). It also allows firms to conduct thorough, fact based analysis of their supply chain, thus providing them with informed knowledge to make strategic decisions involving the supply chain.

Data Integrity/ Information Security Threats

Data and information security risks can largely be managed by the organisation by implemented thorough security checks throughout their data management software. However, in 2001, Ernst & Young (2001) conducted a survey to investigate how many companies had suffered data loss of failure. From interviewing over 250 chief information officers, over 70% of them stated that they had suffered some form of disruption to a critical IT service.

This highlights the issues that data integration is causing many companies across the UK.

To prevent these issues, all organisations should be implementing a variety of security checks and protection systems on their IT systems. Finch (2004) outlines four key systems that all organisations should implement in order to ensure their IT and data integrity. These are;

- Virus detection: All companies should have virus detection software to stop incoming threats from effecting critical IT systems. Furthermore, if this is coupled with a strong firewall, it can block the majority of malicious threats.
- Firewall: A firewall is fundamental to a networks security. Although many companies install a solid firewall on their network systems, they forget that it needs to be managed. This is because the firewall must be updated with security policies, and log files regularly scanned for potential threats.
- Backups: The majority of larger companies will have various backup systems in place to maintain the integrity of data even if a threat occurs. Furthermore, these backups should usually be stored off-site to increase protection. On the other hand, many smaller companies did not recognise the value that back-ups provide.
- User accounts/passwords: Although user accounts and passwords are prominent across the majority of organisations, they must also be constantly managed. This means updated employees access rights, and deleted ex-employees from the system.

Although these systems seem like common knowledge for an organisation to install and implement, it is the careful monitoring and management of the systems that is imperative. Letting a security system become outdated will render it useless, as modern threats will be able to effect critical IT systems. Although risk sources related to data integrity cannot be mitigated entirely, they can be successfully managed through the thorough implementation of numerous security checks (Stoneburner, et al., 2002).

Internal Resource Risks

Internal resource risks has some similarities to data integrity risks, as it involves protecting all the internal resources that are connected within the supply chain. This can include things such as; labour strikes, production failure, IT system failure or insufficient interaction between organisations within the supply chain. Furthermore, similar to the other two risk categories, an organisation must conduct careful planning and preparation to help completely mitigate internal resource risks from occurring. There are a variety of methods in which a company can do, including probability reduction, transferring or sharing risks.

educing the probability of a risk event is often preferred by many organisations, and could be reduced by “ by improving risky operational processes, both internally and in cooperation with suppliers, and to improve related processes, e. g. supplier selection” (Norrman & Jansson, 2004, p. 439). Fundamentally, if a company wishes to reduce the probability of a risk event occurring then they will attempt to integrate all processes with the supply chain. However, although this reduces the probability of a risk event occurring, it is still likely that one will eventually occur, and with full impact.

Another method of reducing internal resource risks is by transferring risk to insurance companies, or supply chain partners. This could be in the form of changing delivery times or suppliers (just-in-time deliveries) or customers (made-to-order manufacturing), or by outsourcing activities (Norrman & Jansson, 2004). Although this is a beneficial method for one company, it could be extremely damaging to the organisation or customer who ends up dealing with the potential risk event. This could fracture supplier and customer relationships, relating in short-term and long-term financial losses for a company.

The final method of reducing internal resource risk is through sharing them. This is usually through the use of contracts, as commercial risks can be shared via these. Furthermore, the internal resource risk could also be minimised through more collaboration throughout the supply chain, as many different departments of the supply chain could absorb the risk effect, thus mitigating it substantially if it were to just impact one process (Cachon, 2002; Tsay, et al., 1998).

On top of these methods, organisations should also be conducting successful supplier relationship management (SRM). SRM can be defined as “ a process involved in managing preferred suppliers and finding new ones whilst reducing costs, making procurement predictable and repeatable, pooling buyer experience and extracting the benefits of supplier partnerships” (Choy, et al., 2002, p. 282). Although this isn’t specifically targeted at managing risk, it has a natural impact to reduce the probability and mitigate the impact of risk. It is similar to the sharing strategy, as it focuses on integrating and collaborating all aspects of the supply chain, to protect

internal resource from potential threats. Furthermore, SRM can reap even greater benefits for an organisation if it is coupled with Customer Relationship Management (CRM). Choy, et al., (2002) studied the effects that integrating SRM and CRM had on Honeywell, a company based in Hong Kong. They found that the collaboration of SRM and CRM had many benefits, as suppliers were more aware of what customers had ordered, and could tailor and increase the quality of products accordingly.

Conclusion

There are many different methods for managing risk, and even though risk events can come in many forms, they all follow similar patterns. An organisation should attempt to mitigate all risk events of occurring by driving the probability of the risk event down to zero, or as close to zero as possible. This can be done through the use of a variety of systems, such as the SCOR framework, which aims to increase the resilience of an organisations supply chain. Furthermore, collaborating and integrating the supply chain has many benefits at mitigating exogenous risk and internal resource risk. This is because it spreads the risk over many different processes, thus reducing the impact on one single function.

As risks can cause significant distress to an organisation and its operations, they must ensure that all the relevant frameworks and theories are being utilised. The type of risk that is going to affect the company is completely dependent on the geographical location of the company and the industry they operate in. This means that one risk management strategy does not work for everyone, and an organisation must ensure they are implementing

the correct risk management strategy to ensure the risk event is mitigated and its effects negated as much as possible.

Bibliography

Berger, P. D., Gerstenfeld, A. & Zeng, A. Z., 2004. How many suppliers are best? A decision-analysis approach. Omega (Oxford), 32(1), pp. 9-15.

Cachon, G., 2002. Supply Chain Coordination with Contract, Philadelphia: The Wharton School of Business.

Chopra, S. & Sodhi, M., 2004. Managing Risk to Avoid Supply-Chain Breakdown. Sloan Management Review, 46(1), pp. 53-61.

Choy, K. L., Lee, W. B. & Lo, V., 2002. Development of a case based intelligent customer–supplier relationship management system. Expert Systems with Applications, 23(1), pp. 281-297.

Ernst & Young, 2001. Information Security Survey 2001, s. l.: Ernst & Young.

Faisal, M., Banwet, D. & Shankar, R., 2006. Mapping supply chains on risk and customer sensitivity dimensions. Industrial Management & Data Systems, 106(6), pp. 878-895.

Finch, P., 2004. Supply Chain Risk Management. Supply Chain Management: An International Journal, 9(2), pp. 183-196.

Gupta, A. & Maranas, C., 2003. Managing demand uncertainty in supply chain planning. Computers and Chemical Engineering, 27(8), pp. 1219-1227.

Huan, S. H., Sheoran, S. K. & Wang, G., 2004. A review and analysis of supply chain operations reference (SCOR) model. Supply Chain Management: An International Journal, 9(1), pp. 23-29.

Juttner, U., Peck, H. & Christopher, M., 2003. Supply Chain Risk Management: Outlining an Agenda for Future Research. International Journal of Logistics : Research & Applications, 6(4), pp. 197-210.

Manuj, I. & Mentzer, J. T., 2008. Global supply chain risk management strategies. International Journal of Physical Distribution & Logistics Management, 38(3), pp. 192-223.

March, J. & Shapira, Z., 1987. Managerial perspectives on risk and risk taking. Management Science, 33(11), pp. 1404-1418.

Norrman, A. & Jansson, U., 2004. Ericsson’s proactive supply chain risk management approach after a serious sub-supplier accident. International Journal of Physical Distribution & Logistics Management, 34(5), pp. 434-456.

Peck, H. et al., 2003. Creating Resilient Supply Chains: A Practical Guide, Bedford: Cranfield University, Cranfield School of Management.

Steele, P. & Court, B., 1996. Profitable Purchasing Strategies: A Manager’s Guide for Improving Organizational Competitiveness through the Skills of Purchasing. 1st ed. London: McGraw Hill.

Stoneburner, G., Goguen, A. & Feringa, A., 2002. Risk Management Guide for Information Technology Systems, Gaithersburg: National Institute of Standards and Technology .

Tsay, A. A., Nahmias, S. & Agrawal, N., 1998. Modelling supply chain contracts: a review. In: Quantitative Models for Supply Chain Management. Norwall: Kluwer Academic, pp. 299-336.

Turney, R., 1996. Risk Assessment in the Process Industries. 2nd ed. Rugby: Institution of Chemical Engineers.