

A framework 01 for understanding risk

OBJECTIVES

This chapter will familiarize the reader with:

- the nature of threat to supply chains;
- how risks can be either ‘internal’ or ‘external’ and how the balance has changed in the past few decades;
- how increasing supply chain complexity and globalization has increased risk;
- methods to quantify risk;
- risk analysis models and understanding of latent threats in the logistics industry;
- the ‘Black Swan’ concept and how this should be used to create resilience;
- the vulnerability of networks and how they interact;
- categories of external supply chain risk.

An analysis of supply chain threats

Corporate risk can come from many sources, sometimes related to the internal production and distribution processes and management of a company, and sometimes from outside. There are many ways of categorizing types of risk, but perhaps the most relevant in terms of supply chain is shown in Figure 1.1.

The first two categories (‘Internal to the firm’ and ‘External to the firm but internal to the supply chain network’) are largely in the control of the

Figure 1.1 Internal and external corporate risks

INTERNAL RISK	Process	Management and value-adding activities
	Control	Rules, systems which govern how a firm controls the processes
SUPPLY CHAIN RISK	External to the firm but Internal to the supply chain network	Demand (downstream) Supply (upstream)
	External to the network	'Environment' (eg natural disasters, weather or socio-political)

SOURCE adapted from Mason-Jones and Towill (1998)

company, but the latter ('External to the network') is largely outside its control, although better intelligence can improve preparedness for disruption.

In terms of supply chain, the last two categories are of most relevance as they relate to threats which specifically affect the extended networks in which most companies in the modern business environment operate.

This is not to say that internal risks of process and control do not impact upon the wider supply chain. One particular issue stems from a lack of visibility upstream and downstream; for example, a large order not anticipated by a supplier could create a bottleneck disrupting supply. Lack of shared information means that many companies are forecast-driven, not demand-driven, and consequently find it difficult to react quickly to changing market conditions, whatever the cause.

The relationship between external and internal supply chain risk is very close. Increasing inventory levels exacerbates risks of redundancy, wastage, shrinkage, financing, and so on, but mitigates external risks (the impact of a disruptive event on supply).

The reverse is also true; reducing internal risks by, for example, unbundling and outsourcing production to remote suppliers leaves companies exposed to a breakdown in the global logistics system or issues of quality control. For example, the problems which Toyota faced in the United States, relating to a malfunctioning brake pedal design, were blamed on a key supply chain partner. One estimate put the total costs of this disaster to

Toyota at \$2 billion, not including lost consumer confidence (Swanekamp, 2010). With 60–70 per cent of a vehicle manufacturer's inventory managed by the supply chain, the management of these risks is business-critical.

While corporate supply chain strategies have been focused over the past few decades on the reduction of internal risk, there has been little realization that what has actually occurred is essentially a trade-off in risk type, not necessarily a complete risk reduction.

This focus has blinkered many companies to the holistic nature of risk. One piece of research suggests that when outsourcing production (and risk), only 10 per cent of manufacturers undertake any sort of risk assessment (Dittman, 2014).

This lack of due diligence, as it might be called, was evident in the implications for supply chains of the 2011 floods in Thailand. Many global companies had allowed themselves to become reliant on high-tech component manufacturers, which were clustered in a remote region where risk was not fully understood. The high-tech sector that developed in Thailand had many comparative advantages in terms of leveraging a local production ecosystem while at the same time offering low-cost labour. The fact that this cluster developed in a region of South East Asia was not the problem; the issue was that a consolidation of specific competences had been allowed to develop in an exposed, flood-prone location.

Figure 1.2 Global supply chain risk – supply chain internal and external characteristics

Supply Chain Characteristic	Internal Risk	External Risk
High stock levels	High	Low
Lean supply chains	Low	High
'Bundled' in-house production	High	Low
'Unbundled' outsourced production	Low	High
Globalized sourcing	Low	High

The severity of threat

Given the complexity and global nature of supply chains, it is increasingly difficult to judge what impact an event will have in terms of disruption. Even a localized event may have massive global implications, as shown by the 2011 Thai floods.

Movements in shipping rates, in contrast, are a global phenomenon. They affect all global supply chains, but although serious, have a less catastrophic impact. A geo-political conflict, depending on where it takes place, could have a very serious, disruptive impact at a global level. A supplier bankruptcy, on the other hand, may be a localized problem, and if contingency plans are in place, may not be serious. Of course, the seriousness of each of these threats is very specific to each supply chain as well as the level of disruptiveness of the event in question.

Is risk increasing?

Rebalancing 'external' and 'internal' risks

External threats to supply chains have received considerable attention following the well-publicized natural disasters in Japan and Thailand. However, understanding of the impacts of these risks is at a very early stage. One survey, undertaken for the World Economic Forum, found that 30 per cent of respondents estimated losses of 5 per cent of annual revenue from supply chain disruption (WEF, 2013a). However, over a quarter of respondents were not able to place any sort of figure on the financial impact.

The risks themselves have not become any more acute. After all, there have always been wars and natural disasters. Rather, it is the evolving supply chain and production strategies of the major global manufacturers that have changed, leading to a rebalancing of the risks inherent in various parts of the supply chain.

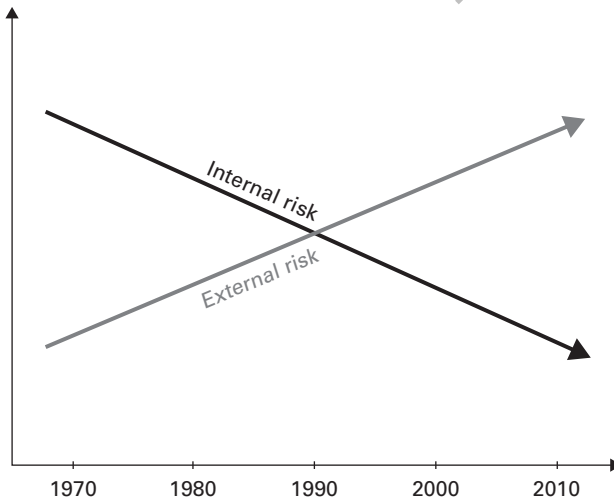
One distinction already discussed above is between 'internal' and 'external' risks. For example, in the 1980s, the personal computer sector adopted traditional manufacturing practices involving the outlay of huge amounts of capital in production equipment and inventory. The risks of this strategy were clear, as many of these companies quickly went out of business when their forecasts proved hopelessly wrong. From this period new business models were developed that allowed manufacturers to focus on design and marketing and let their supplier bear the risk of production.

This process has been referred to as ‘unbundling’ of production. In other words, in this example, ‘internal’ risks were outsourced to contract electronic manufacturers. This, however, did not leave the original equipment manufacturers (OEMs) risk-free – rather, the ‘internal’ risks were transformed into ‘external’, that is, those that are inherent in extended supply chains. The risks have changed in character and, using a medical metaphor, instead of offering a longer-term, chronic threat to corporate health, they are now acute and paroxysmal.

In crude terms, it is possible to say that as inventory holdings have fallen, there has been a proportional diminution in internal risk, but at the same time an increase in vulnerability to exogenous sources of risk. This is not to say that this has to be the case. One of the themes of this book is how to maintain many of the efficiencies that have been achieved in inventory reduction terms while minimizing the increase in external risks.

One example of this relates to the impact of the Japanese tsunami on high-tech supply chains. One consultancy, IHS iSuppli, asserted that the event had had a much smaller effect than would have been expected on the electronics supply chain because inventories had been built up during the prior two quarters as a result of lack of demand in the market (Transport Intelligence, 2011a). It believed that a more widespread disruption was prevented by the level of supplies-on-hand combined with the repair and restart of production facilities and agile moves among manufacturers to shift production from Japan to facilities outside the country.

Figure 1.3 Rebalancing of internal and external risk



Interestingly – and this may have wider implications for other industry sectors – IHS believes that manufacturers may increase orders to buffer against future supply chain disruptions. If this is the case, maintaining higher inventory levels could become the ‘new normal’, a calculated measure deployed to mitigate the disrupting effects of natural disasters and other upheavals.

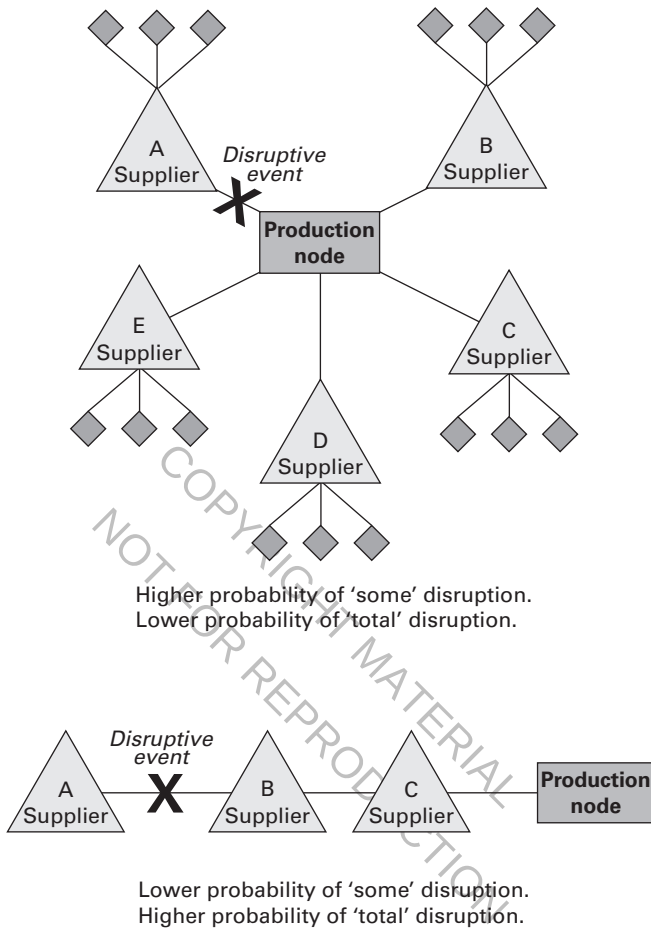
This was also demonstrated by the Chinese automotive sector, which likewise suffered minimal disruption even though several Japanese manufacturers base their production in the country. The reason for this was the lack of adoption of just in time (JIT) delivery schedules, largely because of the poor quality of infrastructure and the lack of a sophisticated supply-side logistics industry that is able to provide these high-value services. This means that Chinese vehicle manufacturers typically keep much more stock on hand than production locations in Japan, North America or Europe.

Outsourcing and unbundling – risk drivers

The ‘unbundling’ of various production processes has led many OEMs to evolve into what are, in effect, managers of integrated and complex networks of remote but interlinked suppliers. In some cases this has produced greater levels of risk, and in others it has had the opposite effect. There is no doubt that extended supply chains are more vulnerable to external threats, but on the other hand, such networks have also dispersed risks to a number of markets by reducing centralization of production.

A small supply chain, for instance, with a single production facility is highly vulnerable to external events, whereas a large, complex supply chain with multiple supplier options has the potential to be much more robust through a greater number of sourcing options. Each option may have higher supply chain risk attached, although – and this is the key point – the probability of overall network disruption is less than in a small supply chain (see Figure 1.4).

The move towards more complex supply chains has its own risks, related to a reduction of visibility and the development of sub-optimal networks. With Asia transforming from a production market to a consumer-led economy, this will only add extra layers of complexity into sourcing and outsourcing decisions for Western manufacturers. Timeliness, reliability, information-sharing, quality and design (along with wider benefits resulting from shared labour skills and knowledge) all need to be weighed along with levels of visibility, management control and, of course, external risk.

Figure 1.4 Global supply chain risk – probability of disruption

Globalization has also created more risks. Extended supply chains mean longer lead times (and less agile response to market conditions), more handoffs between parties, challenges in ensuring quality control, as well as exposure to currency fluctuations, labour disputes, shipping costs, corruption, thefts, natural disasters and geo-political instability. Increased awareness of these threats has led many manufacturers to look at whether they should be adopting a hybrid strategy of remote production combined with near-sourcing in more stable markets closer to the end consumer.

The cost of transport (on which globalization is predicated) is also overlooked as a major risk. This not only includes shipping rates, which have

been volatile over the past few years, but also the cost of fuel, which has been driven up in the past by tension in the Middle East.

The World Economic Forum's Supply Chain and Transport Risk Survey (WEF, 2013a) identified the least effectively managed supply chain components as rated by respondents. The top five are:

- reliance on oil;
- shared information;
- fragmentation along the value chain;
- extensive subcontracting;
- supplier visibility.

As the survey analysis points out, three of these components relate to visibility and control. Improvements in technology can mitigate this type of risk. For example: development of supplier/buyer communities and the use of social media technologies within supply chain communities could be one way in which risks can be reduced; 'sense and respond' technologies allow for greater awareness of the location of products in the supply chain, and hence enable better decision-making/re-routing.

The development of information technologies will play an important role in the mitigation of supply chain threats. There is little prospect that these risks will diminish – some may even increase. Therefore the ability to react to events will become the key competitive differentiator, and technologies that enable an enhanced level of supply chain agility will become highly sought after.

However, the adoption of more technology will also play a role in increasing risks. Increasing reliance on technology will leave supply chains open to 'cyber attacks' or even accidental outages. While technology will lead to greater levels of efficiency, it will also mean that maintaining robust networks will be ever more critical.

Despite this, it is the industry's reliance on oil that is of primary concern to survey respondents. Given the relation between geo-political tension and the price of oil, and the extreme volatility that this causes, it is clear that alternative strategies must be developed. This could entail a rebalancing of the inventory/transportation equation as shippers position stock in closer proximity to end-users. This will increase stock levels, but reduce transport costs. Of course, as mentioned above, this has risks in its own right and these need to be taken into account in a holistic supply chain management strategy. It could also entail a move from global supply chains to near-sourcing of products, especially utilizing less fuel-intensive modes of transport.

The most disruptive supply chain events are those which have not or cannot be planned for. Therefore it is perhaps more useful, rather than look at past events in order to gain some insight into the future, to identify weaknesses in supply chains instead. Addressing vulnerability is the best way to mitigate the impact of a disruption, although there still remains the issue of how much time and money should be invested on each perceived weakness. This approach is called ‘risk-agnostic’ (although a better term would be ‘risk-neutral’) as it prepares supply chains for any type of threat.

Quantifying supply chain risk

It is very difficult to measure the impact of an event on a supply chain and even harder to attempt to forecast the impact of a ‘potential’ event. In many ways it is much easier to work out the costs of holding inventory in the system (the ‘internal’ risk), and address this through a cost-minimization strategy. However, as has been discussed, an assessment of whether or not a company is holding the appropriate level of inventory relies on first quantifying levels of risk.

Many companies are good at working round small and frequent disruptions to their supply chains, without any major cost implication. By their very nature, it is much more difficult to predict low-frequency, low-probability ‘Black Swan’ events, and consequently, making a decision on how much to invest in making a supply chain resilient to these types of events is a challenge.

There are several different ways in which supply chain risk can be quantified. However, one of the simplest ways of measuring risk is by viewing it as the product of the probability of any given event multiplied by its severity (Christopher and Peck, 2004):

$$\text{Risk} = \text{Probability (of a given event)} \times \text{Severity (negative business impact)}$$

A way of measuring the impact of a disruptive event is by tracking the share price of an affected company. Research carried out by the World Economic Forum and Accenture has shown that a company’s share value is impacted by about 7 per cent following the announcement of a supply chain disruption (WEF, 2013a). These disruptions could include natural disasters, production issues, shortage of parts, recalls, and so on. Accenture examined over 62 supply chain disruptions, including the impact of the Japan earthquake and tsunami upon production.

When dealing with risk, manufacturers usually adopt one of three strategies, each of which involves a cost element:

- 1 inventory management – build up safety stock;
- 2 sourcing – developing contingency strategies for specific suppliers or supply chain links;
- 3 ‘acceptance’ – doing nothing as costs of mitigation outweigh benefits.

Deciding on which strategy to adopt relies on understanding the cost implications of each approach. One pharmaceutical company undertook a cost–benefit approach to working out how it should mitigate supply chain risk. It used insurance and industry data to estimate the frequency and duration of disruptions, and using scenario-planning software, analysts worked out how many weeks a year their production would potentially be affected. They were then able to set inventory holdings at a level which would minimize disruption. Of course, the weakness of this approach was that although it minimized disruption, the strategy imposed huge additional costs on the organization, not only from the financing of the additional inventory, but also from the risks of redundancy of stock.

Modelling exercises also need to take into account the length of disruption as well as the probability. There are other variables: for example, the length of time it takes for alternative suppliers to ramp up production. One other interesting factor that impacts significantly on the extent of disruption is the location of the event within the supply chain. The further upstream it occurs, the longer the disruption to supply. The reason for this is that downstream processing locations act as bottlenecks and take time to fulfil back-orders once upstream supply is switched back on.

When attempting to quantify the impact of supply chain disruption, one technique can be to assess the probability of various events taking place. One project undertaken for a consumer packaged goods manufacturer attempted to do this by first categorizing the major threats into three classes:

- natural disasters;
- external disruptions (such as supplier failure);
- internal disruptions (such as fire or IT failure).

The researchers then used a range of publicly available data, as well as that provided by the company, to attribute probability levels to each event. Not only was the probability of an event assessed, but also the duration of such an event with a minimum, maximum and most likely duration figure being arrived at.

In many respects, effective supply chain management is all about the trade-off of one set of risks against another. Keeping higher amounts of stock in various locations is not necessarily a good response to the threat of

disruption as this is not only costly, but in high-tech sectors – for example, where product lifecycles are low – it would be commercially damaging.

Lean supply chains are also a double-edged sword. While they are working efficiently, they have the potential to reduce inventory levels at the same time as maintaining/improving customer service. However, there is no doubt that they are less resilient to external shocks, as they do not provide a safety net when supply chains break down.

In effect, what has happened in the past is that inventory levels have been used as ‘insurance’ against risk. If there have been disruptions to supply or to transportation, ‘safety’ stock has allowed production or sales to continue unaffected. Insurance companies that are now entering the supply chain risk market are allowing manufacturers to outsource this risk, while keeping inventory levels to a minimum. However, quantifying the risk for insurance companies (as well as the manufacturer) is a major challenge.

Understanding the causes of supply chain disruption

Risk analysis and management

In a highly complex environment, involving the interaction of human, technological and environmental factors, it can be difficult to identify the reasons behind an event that leads to supply chain disruption. In order to help risk analysis and management, two academics – Dante Orlandella and James T. Reason of the University of Manchester – developed what has since become known as the Swiss Cheese Model of accident causation.

The original model was developed in the wake of a number of major disasters, which from a transport perspective included the sinking of the Herald of Free Enterprise and the King’s Cross Underground fire. The inquiries into these disasters decided that to understand the causes, it was necessary to understand the context of the event and not just the performance of the employees at the ‘sharp end’. This model was adopted and promoted by the air traffic management regulators and air safety investigators.

The model’s author was in fact developing earlier work that utilized another medical metaphor to explain how a catastrophic event, such as one of those identified above, could occur. Causal factors could lay dormant (like a pathogen in the human body) before combining with other adverse conditions to breach the human defences. In network terms, the auto-immune system is replaced by the procedures and security put in place as barriers to the threat.

Professor Reason made a distinction between ‘active errors’ and ‘latent errors’. The ‘latent errors’ could exist in different parts of an organization’s structure or processes and, after refining the model, Reason said these weaknesses could occur either at ‘organization’, ‘workplace’ or ‘person’ level (Reason, Hollnagel and Paries, 2006).

There was also a change in terminology. Instead of referring to ‘latent errors’, the circumstances that could lead to a disaster were termed ‘latent conditions’. This recognized the fact that in many cases an error could only be defined as such in hindsight. For example, all organizations have budgetary constraints. It is not necessarily possible to predict that reducing funding for one division will result in a catastrophic failure, although that division may have consequent time pressures and poorer equipment than another. All organizations have these latent conditions – on their own they do not result in catastrophic failure. However, what is required is an ‘active failure’ that, when these latent conditions align across a network or organization, triggers a disastrous event. This ‘active failure’ could very well be human error or some sort of violation.

‘Latent errors’ or ‘latent conditions’ exist at various levels. Fallible decisions can be made by senior management and line management can be deficient. Active failures can be made by operatives and inadequate defences to such a concatenation of errors/failures can result in a catastrophic event.

Perhaps one of the most enduring legacies of the model has been a change in mindset when allocating blame for a disaster. It is no longer sufficient to blame an accident or catastrophe on simple human error by a single person, as the context in which that person or event occurred needs to be carefully examined.

In fact, some have argued that the pendulum has swung too much in the other direction. There is a tendency to blame management rather than the ‘human error’ of the operative at the sharp end. Certainly a balance between the two needs to be struck.

What lessons can be learned for supply chains?

The Swiss Cheese Model is relevant to the logistics and supply chain industry at several levels. First, when analysing the causes of a failure within a supply chain, it could be easy to proportion blame to the ‘sharp end’ of an operation without fully understanding the weakness of the entire supply chain.

For example, in this scenario, a road freight operator is a day late in the delivery of an important component to a factory. As a consequence, a production line goes down, costing the manufacturer significant amounts

of money in lost sales and idle labour. Who is at fault? The obvious party to blame is the trucking company that failed to deliver on time, resulting in a major supply chain failure. This could be due to a breakdown en route, human error in the dispatch department or inability to locate the goods in the warehouse due to incorrect put-away.

However, a more holistic analysis along the lines of the Swiss Cheese Model goes a lot deeper. For example, senior management of the manufacturer may have recently insisted on a 'lean' inventory reduction programme to eliminate 'waste' and bring down working capital tied up in stock-on-hand. Along with that, in our scenario, the purchasing department had come under pressure to reduce costs by outsourcing production to a cheaper supplier abroad. Supply chain managers had instituted a 'just-in-time' delivery schedule with this supplier.

However, there had been significant quality issues with the components produced by the supplier, which had resulted in an earlier delivery of goods being rejected. Instead of using an express parcels company to deliver the urgent consignment, with the added benefit of being able to track the goods in transit, the manufacturer's cost reduction programme had meant that only 'standard' road freight services could be used. The haulier that had been chosen had committed to levels of service that it wasn't able to fulfil, because of the low margins it was making on the contract. Consequently, the shipment arrived late.

In terms of the Swiss Cheese Model, there are some obvious latent conditions that exist in this scenario:

- Senior management had decided on a policy of inventory reduction in order to free up working capital and minimize waste.
- Management had also outsourced production to a low-cost supplier based remotely, as a way of cutting manufacturing costs.
- Logistics managers had negotiated transport costs down and implemented a policy to utilize non-premium services.

In isolation none of these three latent conditions could be seen as 'errors'. In fact, supply chain theory and practice has over the past three decades promoted these measures. However, they have created an environment in which the 'active error' of the trucking company has brought about a major loss to the company.

What is also lacking from this company's resilience is any 'defence' to this failure of supply chain execution. In fact the obvious 'defence', that is, an element of redundancy in supply chain inventory, has been eroded by management.

Other ‘defences’ could have focused around quality control. To what extent was the supplier’s processes and product checked before production was outsourced? The same issue with quality applies to the transport provider. Where were the checks and balances when the logistics contract was awarded? Was the financial health of the haulier monitored?

There is no single point of blame. Was it the untrained driver’s fault for failing to finish his delivery schedule? Was it the road haulier’s fault for not providing sufficient training? Or was it the customer’s fault for negotiating the haulier’s rates down so far that it couldn’t afford to pay experienced driving staff?

Was it, in fact, the fault of the supplier, whose failure to ship error-free goods in the first place was a major causal factor? Or the line management who chose the supplier – or in fact the senior management who decided on this outsourcing strategy in the first place, without sufficient oversight?

A summary of the supply chain failure event outlined above could be laid out as follows:

Corporate level: organization and management issues (latent)

- management forced into adopting cost-driven outsourced production strategy without necessary oversight;
- no clear understanding of cost implications of supply chain failure;
- narrow, silo approach to cost reduction undertaken.

Line management issues (latent)

- logistics managers overly focused on transport cost reductions, not quality;
- purchasing managers likewise focused on input component costs, not quality;
- freight operator management forced to compete on small margins, resulting in hiring of untrained staff;
- supplier quality control flawed.

Local issues (active)

- Driver fails to complete delivery schedule.

Flawed safety nets

- quality control programme insufficient;
- supply chain visibility insufficient;
- inventory control flawed;
- freight operator had no telematics or transport management system in place.

Developing resilience to ‘network events’

In his seminal work *The Black Swan* (2007), philosopher Nicholas Taleb asserts that most business professionals assume we live in a world of mild randomness, where events don’t stray far from the mean.

Contrary to this view, Taleb argues that, because of tightly integrated markets and networks, we live in periods of wild randomness where small probability events carry major consequences. Intertwined networks – energy, transport, financial, ICT and human – mean that the consequences of failure in one can be critical and unforeseen in another.

From the enormous complexity of the relationships between the various networks outlined, it is obvious that no organization or government could plan for any one catastrophic event. These events are variously referred to as ‘high impact–low probability’ (HILP) or ‘Black Swans’.

However, this is not an excuse to do nothing. Instead, managers and planners should focus on making operations and supply chains resilient to all shocks, not just to those that they believe (usually erroneously) may happen.

In a report on the Icelandic volcano crisis of 2010, research organization Chatham House classified risk into three categories (Lee and Preston, with Green, 2012):

- 1 ‘Black Swans’ – these are the ‘unknown unknowns’ that are impossible to predict but that have the potential to do major damage to economies and businesses. While planning for a specific event is impossible, it is possible to build general resilience.
- 2 ‘Known and prepared for’ – these events have occurred in the past, such as a pandemic or flood, and are expected to happen again in the future, although at a time and place unknown. A large degree of preparedness can be achieved, and the debate is usually about the level of resources that should be committed.

- 3 'Known and unprepared for' – this scenario could involve events that have been foreseen but for which governments or businesses have discounted 'worst-case scenarios'. This is obviously a misjudgement for which there are political or commercial consequences.

Understanding network failure

Networks have attained critical importance to the supply chain industry. Whereas the simple Swiss Cheese Model discussed above looked at largely internal dynamics and decision-making processes, networks would be described as being external influencers. However, the model also works when exploring the interrelation between networks and their impact on supply chains, and indeed the wider economy and society.

Energy networks

In the developed world the power grid is essential to every part of the economy and society. In some parts of the world, where it is not in existence or unreliable, contingencies are put in place should it fail. This will include back-up generators, which are widely used in markets such as India.

In a supply chain perspective, electricity is essential for powering warehouses but also traffic signals and even petrol pumps. As well as providing light, it also powers information and communications technology, including mobile networks. The dependence on a reliable energy source makes the supply chain and logistics sector highly vulnerable to power cuts.

Human networks

Human networks are rarely analysed in terms of risk to supply chains. However, with the logistics and transport industry so labour-intensive, the human angle is clearly a key vulnerability.

How many companies would be able to operate efficiently or at all if half of their workforce did not turn up for work? This would have major implications, especially for grocery retailers, who rely on regular and frequent deliveries to their stores. It would also disrupt supplies on petrol to filling stations, medical supplies to hospitals, the delivery of coal to power stations, and so on.

Information and communications technology

ICT networks underpin much of the modern supply chain and logistics industry, providing visibility into warehouses, enabling efficient transport

management, GPS data, facilitating communications between shipper, logistics provider, end-user, customs and border controls, to name just a few uses. In addition to this, it is essential for air traffic control, traffic management in urban areas and port community systems.

With the industry becoming ever more reliant on ICT, any length of downtime becomes critical to efficiency and safety. As advanced telematics becomes entrenched in vehicle control systems – such as ground-to-air communication and eventually car-to-car (as part of intelligent transport systems) – this vulnerability will only become more important.

Transport

The term ‘transport network’ can refer to both the physical infrastructure and the flows of traffic across the infrastructure. It could also be said that there is a further ‘organizational’ element, with some passengers (those not moving by car) and all cargo being managed by service providers (either air, sea, road or rail). This is important from a risk perspective as businesses moving goods and passengers interact more closely with other networks, such as ICT, in the normal pursuit of their business.

The various networks interact with each other at nodes, as in many cases journeys are multi-modal in nature. For example, the commute to work will often involve a journey to a railway station by car, a train journey and perhaps a bus at the destination. Likewise, air cargo is almost always moved to the airport by road.

The nodes, which are an essential part of passenger and freight movements, are by their nature bottlenecks and highly vulnerable. In the shipping sector in particular traffic is becoming increasingly concentrated on a diminishing number of nodes (ports), which is increasing the risk.

This concentration of risk is also occurring in some prime locations that have developed multiple nodes. For example, Dubai has developed a major port and airport. Louisville in the United States is at a confluence of rail, road and air networks. In Europe, the Randstad region of the Netherlands includes the Port of Rotterdam, Amsterdam Schiphol Airport as well as road and rail networks that link the region with the rest of Europe. The air, road and rail networks are also intensively used by passengers in this highly populated urban area.

The mode most vulnerable to disruption has proved to be air travel. Perhaps because most air cargo travels on the same aircraft as passengers, it is particularly at risk from trends and developments affecting passenger travel as well as its own industry dynamics. For example, the SARS crisis of

2003 impacted on air cargo capacity as passenger flights were cut, due to the downturn in the numbers of people travelling to Asia. This dynamic is of considerable importance to the global economy. It is estimated that about a third of manufactured goods, in terms of value, are shipped by air and 55 per cent of the UK's exports to non-EU countries is airfreighted.

The type of goods moved by air is also important, as these often have a critical impact on other networks. These include medical (equipment and vaccines, for example) and electronic integrated components for telecoms networks.

How are networks interconnected?

Understanding the wider impact of a disruptive event is made more difficult as it is impossible to view individual networks in isolation. Increasingly networks are interwoven and interconnected in ways that have become increasingly difficult to map or understand.

If, for example, there was a terrorist attack on a part of an urban metro system, it would be likely that the decision would be made to shut down the whole of this particular network. Passengers would exit onto the streets, and many would then use their mobile phones, potentially overloading the mobile telecoms network. Websites would be bombarded with enquiries, and the heavy volumes could bring down the internet. With news spreading, traffic chaos would not just be restricted to the inner urban area but would spread out to orbital roads and the major motorway interchanges. Overland train stations would be overwhelmed by commuters trying to get out of the city early. Economic and humanitarian damage could be considerable. This is not an imaginary scenario as this actually occurred after the 7 July bombings in London in 2005.

Another example relates to the electricity networks and their role in underpinning pretty much every other network in the UK – mobile networks, financial markets, IT, lighting, the traffic signals on the road and rail. With electricity down, garages cannot operate and trucks, cars and ambulances are not able to fill up with petrol. As has been seen in New York during the Superstorm Sandy disaster, when the power goes out, life comes to a halt.

The critical nature of the electricity power supply has not gone unnoticed by malign forces. The technology systems of the main power and distribution companies are consistently under attack – and there was even a threat by one group to black out the opening ceremony of the London Olympics in 2012.

However, a significant crisis came from another source. When temperatures fell to below -15 degrees Celsius in the winter of 2010, there was a threat to the infrastructure of electricity sub-stations. It needed large numbers of engineers to physically defrost critical components. This meant that at a time of crisis to one network, additional stress was placed on another – the human network.

The obvious question is, what would happen if the UK had been in the middle of a swine flu pandemic at the time of the severe weather and this meant that half of the engineers hadn't been able to show up to work? This could be termed an 'alignment of vulnerabilities', as identified in the Swiss Cheese Model, which means that when multiple events coincide (and these on their own need not be critical), networks can topple one after another.

External risk categories

It is possible to divide external threats into five main categories, each of which is dealt with in detail within this book.

Environmental

Natural disasters

This category comprises a wide range of disruptive events, including extreme weather, earthquakes, tsunamis, floods and even volcanic eruptions. The economic cost of natural disasters was estimated by insurance company Swiss Re at \$158 billion in 2016 (Swiss Re, 2016). The supply chain consequences are derived from not only the disruption of production but also the impact on transportation services and infrastructure. A World Economic Forum (WEF)/Accenture study found that, following the Japanese tsunami/earthquake, the operating profits of 15 leading multinationals fell by 33 per cent in the subsequent financial quarter directly as a result of supply chain disruption (WEF, 2012).

Climate change

Within this category, longer-term environmental issues can also be placed. The survey conducted by WEF specifically identified 'rising greenhouse gas emissions' and 'failure of climate change adaptation' as the major issues of concern for company executives. The WEF pointed out that even in the wake of major natural disasters, such as the Japanese tsunami, man-made

disasters such as ‘mismanaged urbanization’ were more likely to be disruptive in the next 10 years than earthquakes and volcanic eruptions.

Pandemics

Pandemics may not be the first risk identified by supply chain managers, but they are one of the most serious. In the last instance of an outbreak in summer 2009, the swine flu virus killed 392 people, although in fact it could have been much worse. At the beginning of the crisis the UK government was warning of a potential 65,000 fatalities. One assumption made by government agencies is that if a flu pandemic takes hold, up to 50 per cent of the workforce could be affected, with each person who falls sick taking between five and eight days off work (Department of Health, 2013). This would have immediate impact on the ability of the private and public sector to maintain operations, especially in such a labour-intensive industry as transport and logistics. The swine flu outbreak of 2009 provided a very real warning of what could happen and the potential impact on the UK’s society and economy.

These risks are dealt with in more detail in Chapter 4.

Economic

In recent years the issue of supply chain risk has been placed firmly on the corporate agenda by a confluence of natural disasters and terrorist actions. However, the focus of risk upon ‘spectacular’ events means that other causal factors can be overlooked. In fact, the WEF survey referenced above found that the most important network vulnerability identified by respondents related to the cost of oil. Other economic risks are also viewed as highly important – more so, for example, than extreme weather or terrorism.

Demand shocks

One of the most pressing supply chain risks from an economic perspective is what can be termed ‘demand shocks’. An example of this is the disruption caused by the company failure of suppliers following the 2008 recession. This was particularly relevant to the high-tech and automotive sectors, where supplier bankruptcy was widespread. Many of the problems were caused by manufacturers ‘switching off’ supply from remote suppliers, and although this had a short-term positive effect on inventories and balances, it meant that when demand picked up strongly in 2010, manufacturers were unable to meet demand.

Manufacturers are ever more exposed to currency risks given the globalized nature of their suppliers and customers. Given the debt crises of many economies and the impact this is having on the strength of the euro, dollar and other currencies, this risk is likely to continue in the coming years.

Within this category the WEF survey identified 'chronic fiscal imbalances' as the key risk. This was linked to the possibility of systemic financial failure throughout the world. This would have obvious impacts for supply chains, not least related to the collapse of suppliers and the inability to access trade finance. Volatile currencies are also unhelpful to the development of trade.

Supply shocks

'Supply shocks' are less obvious, but material threats all the same. The volatile nature of shipping rates could fall into this category. In early 2012 shipping rates on Asia–Europe routes increased by about \$1,000 per TEU (from about \$650 to \$1,650) – a situation that most shippers would find difficult if not impossible to predict.

Oil

Volatility in the oil market has a direct impact on the supply costs of shippers, whether they operate on a national or international basis. In most developed markets, fuel accounts for around a quarter to a third of transport operating costs and a fluctuation in these costs has a major influence over sourcing and distribution strategy decisions. A surge in the price of oil would certainly rebalance the near-sourcing/offshoring debate in favour of the former and it would also encourage more distributed inventory holding strategies, as opposed to the centralization of stock that most companies choose today.

The risks to supply chains are not necessarily derived from a steady rise in the price of oil – manufacturers and retailers can plan for this eventuality. However, a sudden spike in oil costs caused, for example, by a crisis in the Middle East would be a much more serious threat as this would have major implications in terms of profitability and modal choice.

Trade disruption/border delays

The success of the World Trade Organization, the advent of the Single European Market and the North American Free Trade Area (NAFTA) has had a major impact in facilitating trade flows and enabling the global supply chain phenomenon. However, as manufacturers and retailers source goods from increasingly far afield, accessing markets without good governance and trade relations, the issue of disruption to trade becomes more significant.

One of the problems that companies face is the unpredictability of such delays. A lack of standardization of documentation and harmonization of trade regulations in Africa is particularly disruptive to the smooth running of trade networks. High levels of bureaucracy increases the probability of errors delaying shipments. Integration into global supply chains relies on not only visibility of supply but also reliability.

Another potential risk to importers and exporters is the incidence of trade wars. The WTO handles a considerable number of disputes a year between members, and the mechanisms that it provides for dispute resolution have been a major factor in preventing more significant breakdown in trading relations. However, tensions, particularly between China and the United States and the EU, continually run high, as protectionist elements lobby governments to protect manufacturing from cheap imports. As markets come under increasing economic pressure, the calls for more barriers to trade will also grow, to the detriment of global supply chains.

Industrial action

A rise in work stoppages and slowdowns throughout the world is having a significant impact on supply chains. To illustrate the vulnerability of the global transport and logistics sector to this threat, the ports at Antwerp and Rotterdam, Frankfurt International Airport, Brazilian customs agents, Costa Rican port workers and Korean truck drivers have all been on strike at some point in the recent past.

As a result, many shippers now diversify their shipments across several modes and gateways so as not to be completely exposed by any disruption. For example, US shippers (who have a great deal of experience of the impact of industrial action at North American ports) are now better able to divert volumes to unaffected gateways. If there are disturbances at East and Gulf Coast ports, for instance, they can utilize West Coast as well as Canadian and Mexican ports, which are linked to the US heartland via a growing rail and intermodal system.

Work stoppages or slowdowns are amongst the most important supply chain risks that companies need to account for and manage accordingly. However, with the continued economic uncertainty throughout the world, this will prove difficult as labour unions fight to maintain existing jobs in ports and other transportation nodes. This will likely create a vicious cycle as strikes, as seen in the past, can easily cripple an economy – thus further exacerbating an already difficult situation.

These economic risks are dealt with in more detail in Chapter 6.

Societal risks

Corporate and social responsibility

Supply chains have expanded into many emerging markets where the workforce and the environment are much more vulnerable to exploitation than in the developed world. Companies such as Apple have been accused of taking advantage of low-cost labour and lack of environmental regulations to manufacture their products more cheaply and efficiently than they could in North America or Europe.

The risk emanating from their supply chains in this instance is primarily reputational, although of course if enough consumers were to boycott their products, there would also be a financial impact. For example, considerable damage was done to the brands of several Western retailers following the Rana Plaza fire in Bangladesh in 2013. More than ever, global companies are being forced to take responsibility for their suppliers.

Of course this is easier said than done. In many cases, manufacturers and retailers are not aware of their lower-tier suppliers. Pressure regarding working conditions, the environment and even the use of conflict minerals means that much more consideration is being placed on visibility up the supply chain. In many cases this has resulted in companies undertaking audits of their suppliers for the first time. The indirect benefit of this has been that companies have been able to identify weaknesses in their supply chain, such as single sourcing issues.

These risks are dealt with in more detail in Chapter 7.

Security

Geo-political tension

There are many flashpoints of geo-political tension around the world: the Korean peninsula; Taiwan and China; various territorial disputes between China, Japan and the Philippines, to name just a few. However, perhaps the most worrying in terms of actual supply chain risk is the Middle East. The Arab Spring created instability throughout the region, with particular implications for one of its biggest economies, Egypt. In addition, sanctions against Iran led to threats by the country's leaders to shut the Strait of Hormuz through which much of the world's oil supply passes. Bellicose announcements by the new Trump administration in the United States could destabilize the region once more.

Terrorism also falls into this category, the most obvious sources being Al-Qaeda, its Somalia-based affiliate, Al-Shabaab, and more latterly the

so-called 'Islamic State'. Some analysts believe that the more successful the war being waged against ISIS in Syria and Iraq, the greater the likelihood that the organization will adopt terrorist tactics and export the war to Europe and North America.

Risks to the supply chain come not only from the terrorists (such as the Yemen parcel bombs infiltrated into the air cargo system in 2010), but also from regulators seeking to limit the impact of a terrorist event by increasing levels of security-driven regulations and procedures. Despite seeming counterproductive, it is a typically politically expedient response to a crisis.

Cargo crime

In parts of the world, a breakdown of law and order has made shipments of goods highly vulnerable to theft by criminal gangs. Even in developed countries in North America and the EU, the problem is very significant. The response of the law enforcement agencies is often weak because of the low priority afforded to the problem by politicians and a lack of responsibility by police; the misdemeanour often straddles different geographies, and in most countries 'cargo crime' itself has no separate legal status. Hence few resources are allocated to tackling the problem.

Shipments are rarely stolen while physically moving (although hijacking vehicles while in motion is becoming more prevalent). Instead, they are most vulnerable in warehouses, airports, ports, intermodal yards or while a driver is taking a break.

Corruption

Corruption costs shippers billions of dollars a year, and while it is most widespread in markets such as those in West Africa, various forms of it are systemic to the logistics industry right across the world. The best-known form of corruption is the bribery needed to facilitate the transit of goods across international borders. Customs officers are badly paid in many countries, and augment their meagre salaries with this additional form of revenue. Links with organized crime can be strong to make sure that illegal goods are not inspected or seized.

However, much more money can be made by mis-declaring the duties that should be paid by importers, and this often involves large numbers of customs officers at all levels. Either directly or indirectly, shippers have to pay the cost of corruption, and an increasing expansion into emerging markets, either as import or export markets, will increase their exposure to corruption and criminality further.

Piracy

Piracy can also be a major issue for supply chains, although the true cost of the disruption is largely hidden. For instance, although millions of dollars were paid to pirates off the Somali coast (with ransom activity reaching a peak in 2011), the majority of supply chain costs occurred when shipping lines were forced to divert to longer routes in order to avoid the problem areas. Other costs include increased insurance; security and guards; increased steaming speeds; higher wages for seamen (danger money); not to mention indirect payments for military operations.

A coordinated response by the international community saw piracy in Somalia reduce dramatically. However, new areas of threat have since sprung up – especially in the waters off Nigeria. As this market develops and becomes of greater interest to multinational shippers, the problem is set to grow worse.

These risks are dealt with in more detail in Chapters 8, 9 and 12.

Technological

Technology failure/outage is a major concern to shippers, although as yet there have been few significant incidents (at least that have been revealed). A lot of money has been spent by agencies, such as the Pentagon, in assessing and planning for a ‘cyber terrorist’ attack, although minor disruption to date has come from power failures or accidents. More reliance in the future will be placed on information and communications networks as the supply chain industry becomes increasingly paperless, and this will only heighten the risks. However, actually measuring the true nature of the threat and robustness of information systems is difficult.

The WEF survey found that, in terms of technological risks, critical systems failures were deemed to have the highest potential impact. However, cyber-attacks were identified as being most probable, either from a state-sponsored, criminal or terrorist source. Other risk events included ‘massive digital misinformation’, ‘incidence of data fraud and theft’ and ‘failure of intellectual property regime’.

Cyber-crime is dealt with in Chapter 9 as part of a wider examination of criminal activity.

CASE STUDY South Africa

A 2011 survey designed to identify the key risks to the supply chain in South Africa has highlighted power outages, theft and labour disputes as the primary concerns. The survey also studied the different types of risk management strategies that are currently in place in the country.

The MIT Center for Transportation and Logistics Global Risk Survey was undertaken in South Africa jointly by the Association for Operations Management of Southern Africa (SAPICS) and IMPERIAL Logistics, in collaboration with MIT (MIT, 2011).

The survey found that extended loss of electricity is five times more likely to occur in South Africa, compared with the world average. Employee theft/executive misdeeds come in four times higher than the international average. Protracted labour disputes are 2.5 times more likely to transpire and disease/inflation 2.3 times higher.

Interestingly, the survey found that, in terms of the top 10 supply chain risk factors, South Africa is more closely aligned to developed rather than developing economies. However, extended electricity loss and major software systems failure are two challenges more commonly associated with developing economies.

South African companies rated raw material supplier failure as the top supply chain risk, followed by finished goods manufacturing failure, product quality failure, transportation carrier failure and economic recession/market collapse. 'Notably, within South African supply chains, companies tend to work more with customers than suppliers in addressing risk management,' said Abrie de Swardt, IMPERIAL Logistics Marketing Director.

In terms of risk mitigation perceptions, South African companies believe in a local response over a central risk response action. This falls in between the North American and European approaches, as identified by the global survey findings. 'By addressing supply chain risk through a centralized approach, a company aligns its strategies to the holistic context. Response at a local level allows site level staff to apply their own actions immediately,' added Abrie de Swardt.

Summary

The character of corporate risk has changed dramatically over the past few decades. Companies have successfully reduced internal risks by limiting inventory levels and improving production quality. However, external risks have been increased through longer, more complex supply chains that rely on suppliers and transport partners to succeed. The understanding of these types of risks is at an early stage. Supply chains need to be made more resilient to 'Black Swan' events and managers need to adopt agile and adaptive strategies to cope with the unpredictable and volatile nature of the modern world.

Key points

- Over the past few decades, 'internal' production and inventory risk has reduced while 'external' risk within supply chains has increased.
- Risk is measured as a function of the probability of an event and its likely severity.
- The Swiss Cheese Model of accident causation is commonly used to analyse risk and risk management.
- 'Black Swan' events (those with small probability) are having increasing impact on supply chains because of the interconnected nature of modern networks.
- Supply chains need to be 'risk-agnostic', that is, resilient enough to cope with any eventualities.
- External risks can be categorized as follows: environmental, economic, societal, security and technological.