

# Identifying and Managing Supply-Chain Vulnerability

by Paul Chapman, Martin Christopher, Uta Jüttner, Helen Peck and Richard Wilding

**Recent events have highlighted the risk that surrounds many supply-chain operations. Markets have become more volatile and hence less predictable. Global sourcing strategies have extended supply pipelines and the widespread adoption of Just-in-Time practices has increased the vulnerability of supply-chains.**

Modern supply-chains are very complex, with many parallel physical and information flows occurring in order to ensure that products are delivered in the right quantities, to the right place in a cost-effective manner. Consequently, **supply networks** may be a more accurate term than supply-chains.

The drive towards more efficient supply networks during recent years has resulted in these networks becoming more vulnerable to disruption. In particular, there often tends to be very little inventory in the system to 'buffer' interruptions in supply and, therefore, any disruptions can have a rapid impact across the supply networks.

These disruptions can arise from a number of sources, for example:

- Natural disasters – for example, the Kobe earthquake, which affected supply networks across the globe; or, more recently, foot and mouth disease, which has affected the UK's livestock haulage industry, tourist industry and other sectors
- Terrorist incidents – for example, events in the USA on 11th September 2001
- Industrial or direct action – for example, the fuel price protest of September 2000, which very rapidly impacted on almost every supply network in the UK
- Accidents – for example, a fire in a component supplier can have such a serious impact on a manufacturer that they are forced to shut down operations, such as Toyota in 1997 – due to problems at its supplier of brake-fluid proportioning valves
- Operational difficulties – for example, production or supply problems at one supplier can impact every organisation in the supply network

Owing to the close interrelationships between many supply networks, the impact of such disruptions can be far reaching.

When chassis manufacturer UPF Thompson became insolvent at the end of 2001, the

impact upon its major customer, Land Rover, was sudden and severe. UPF Thompson was the sole supplier of chassis for the Land Rover Discovery, and receivers KPMG threatened to halt supply unless Land Rover made an immediate up-front payment of between £35 million and £45 million. KPMG justified its actions by pointing out that it was legally obliged to recover money on behalf of creditors and the sole supplier agreement represented a valuable asset. A recent court ruling had determined that receivers were legally entitled to exploit a customer's vulnerability for the benefit of creditors. Land Rover faced the possibility of having to suspend production of the Discovery, until a temporary injunction was secured granting the carmaker a short-term reprieve. The injunction averted the lay-off of 1,400 workers at its Solihull plant, plus many more amongst Land Rover's network of suppliers.

## Research Pilot Study

The robustness of supply networks is thus recognised as being critical for individual organisations and for the economy as a whole. To aid our understanding of the extent to which supply vulnerability is recognised and understood by industry, Cranfield Centre for Logistics and Transportation was commissioned by DTLR, DTI and the Home Office to conduct a pilot study. The aim of this research was to examine the state of knowledge, and 'best', or 'current', practice in the supply-chain risk management and business continuity arenas.

On an individual firm basis, companies have been aware of the need for disaster recovery and crisis management for some considerable time, particularly in areas such as information technology and production facilities. Furthermore, business risk and continuity management is now receiving increasing attention by companies – and their insurers, particularly as regards the loss of market share and the time, and cost, of re-entering a market after a significant disruption to supply. »

### Risk in the Supply-Chain

The concept of the supply-chain as a network of interrelated entities that combine to enable the satisfaction of customer demand is well established.

However, for many, if not the majority of, ultimate consumers, their knowledge and understanding of supply-chains is limited. Even amongst those who work in industry and commerce, unless their responsibilities lie within the specific functions that are touched upon by the supply-chain, that knowledge is usually only sketchy.

Given the complexity of today's typical supply-chain networks, this lack of knowledge is not surprising. Yet, as we will argue, the complexity of the chain – which is tending to increase rather than diminish – brings with it higher levels of risk and hence vulnerability.

Supply-chains that comprise hundreds, or possibly thousands, of companies, extending over several tiers, present numerous risks. Broadly, those risks can be classified into two types: risks **arising within** the supply-chain and risks **external** to it.

“... the most apparently secure and stable of supply-chains can become vulnerable to changes in the nature of a relationship, or unforeseen changes in the environment.”

Risk within the supply-chain arises from interaction between constituent organisations across the supply-chain. It is caused by sub-optimal interaction and co-operation between the entities along the chain. Such supply-chain risks result from a lack of visibility, lack of ‘ownership’, self-imposed ‘chaos’, the misapplication of Just-in-Time practices and inaccurate forecasts.

Where these interactions occur in successive echelons in the supply-chain we have called them ‘serial’ interactions. However, there is clear evidence for another type of interaction between participants in supply-chains; and since these can occur within a single echelon, we have termed these ‘parallel interactions’. The phenomenon is observed quite commonly in multi-product, manufacture-and-assembly firms, such as the motor industry, domestic appliance and some aerospace companies. It results from the need to make changes to the product mix, usually at a late stage in the planning cycle, often because a first-tier supplier fails to deliver the ordered quantity,

resulting in rescheduling and the customer changing the requirements placed on other first-tier suppliers.

There are also examples of parallel interactions in retail supply-chains. Stockouts in one product group lead to switching to other groups – for example, from traditional white sliced bread to brown bread. The recent foot and mouth crisis created multiple parallel interactions at a supply-chain level – at one brewery production was halted because the waste material could not be disposed of, a small rugby ball manufacturer ceased production because of a shortage of leather and even a steam railway was impacted because the coal used in locomotives was being used to burn carcasses. Parallel interactions can be exacerbated by the aims of holding low inventories and achieving high resource utilisation. Suppliers in a parallel supply-chain, which at first would seem unrelated, can be affected by such occurrences.

External risks arise from interactions between the supply-chain and its environment. Such interactions include disruptions caused by strikes, terrorism and natural catastrophes. Any disruption at any stage in a supply-chain that can be linked to environmental causes is ascribable to external risks.

### Definition

Together, supply-chain risks and external risks threaten the continuity of supply-chain operations. In addition, although supply-chain risks and external risks have independent sources, simultaneous occurrence of both intensifies the damage. The impact of these threats will depend upon the way the supply-chain is structured, such as the contractual relationships between organisations. Thus, **supply-chain vulnerability** can be defined as: ‘An exposure to serious disturbance, arising from risks within the supply-chain as well as risks external to the supply-chain.’

The Land Rover example illustrates that even the most apparently secure and stable of supply-chains can become vulnerable to changes in the nature of a relationship, or unforeseen changes in the environment. In this instance, it was the financial collapse of a trading partner compounded by a change in the regulatory environment, together with the leanness of Land Rover's inbound supply network, that magnified its susceptibility to damage.



The '3-P' Approach of: Philosophy; Principles; Processes

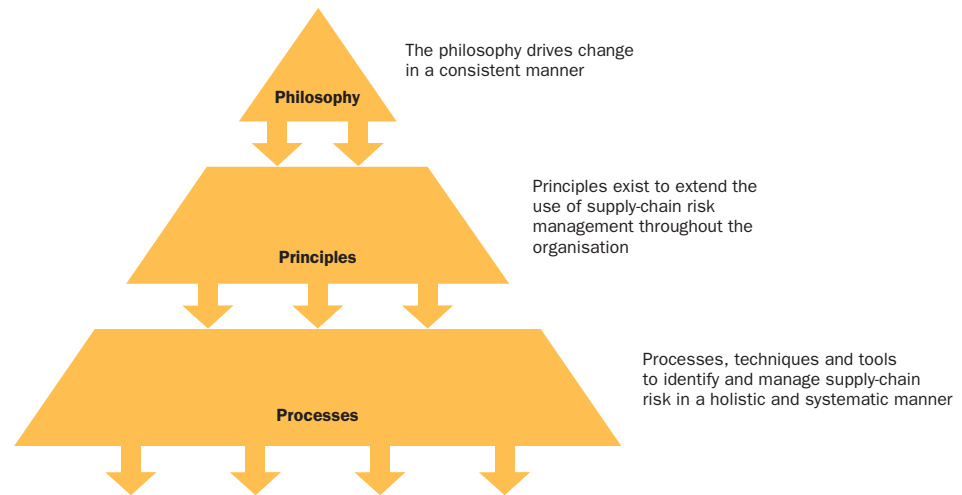


Figure 1

“In effect, current understanding is underdeveloped and only capable of looking at pieces of the supply-chain vulnerability jigsaw, without the ability to connect those pieces and see the wider picture.”

**Supply-chain risk management** aims to identify the areas of potential risk and implement appropriate actions to contain that risk. It can be defined as: ‘The identification and management of risks within the supply-chain and risks external to it, through a co-ordinated approach amongst supply-chain members, to reduce supply-chain vulnerability as a whole.’

Industry associations such as The Institute of Logistics and Transport have an important role to play here in promoting awareness of supply-chain vulnerability. They are also uniquely placed to foster greater co-operation within industry and between industry and government.

**Key Findings**

The key findings from this first phase of research into supply-chain vulnerabilities are:

- Supply-chain vulnerability is an important business issue
- Little research has been undertaken into supply-chain vulnerabilities
- Awareness of the subject is poor
- There is a need for a methodology for managing supply-chain vulnerability

Recent events demonstrated and highlighted that supply-chain disruptions can have a major impact upon advanced, industrialised economies. Whilst these were exceptional events, this research uncovered numerous, smaller scale incidents capable of creating wide-ranging and unforeseen disruption.

On the one hand, contemporary developments in business thinking have, in many instances, reduced supply-chain vulnerability to

‘everyday’ commercial supply-chain risks by improving their internal efficiency. However, these same measures have reduced resilience to ‘exceptional’ external disruptions.

Whilst many of the concepts behind the prevailing trends in supply-chain management appear sound in themselves, unanticipated side effects again point to a lack of understanding of the true nature of modern supply-chains and their vulnerabilities. The findings of this research underline the fact that these increasingly lengthy supply-chains are, in truth, supply networks connecting businesses, industries and economies. Consequently, the diverse range of effects triggered by even a modest incident can fail to lead to underlying weaknesses being diagnosed if they are considered only in isolation and not as part of the wider, overarching system. In effect, current understanding is underdeveloped and only capable of looking at pieces of the supply-chain vulnerability jigsaw, without the ability to connect those pieces and see the wider picture.

Business continuity and risk management, particularly with regard to information systems, appears to be fairly well understood and applied within individual organisations. The same is not true in terms of risk management in supply-chains. Where awareness exists, a major impediment to the application of supply-chain continuity management is the lack of an integrated programme of action or access to an appropriate managerial ‘toolkit’.



With the need for a toolkit in mind, the research went on to look at the issue of supply-chain risk management at three levels. The report suggests that dealing with supply-chain vulnerability appears to require a change management approach; that is, one that employs the '3-P' approach of: Philosophy; Principles; and Processes, see Figure 1, on the previous page.

Such an approach recognises that the 'right' 'Philosophy' for tackling supply-chain vulnerability depends on the culture, structure and business drivers dominant in an industry sector.

Philosophical issues are important because they drive change. These broad beliefs drive change in a consistent manner, be it in the short-term or the long-term. For example, organisations that embrace Total Quality Management (TQM) have a fundamental belief in the need to utilise and develop all the capabilities of all their employees. From a supply-chain vulnerability perspective, further work needs to be undertaken to understand how the fundamental beliefs of organisations influence how they respond to the need to manage risk and continuity. Nevertheless, it was possible to identify four issues that, at the philosophical level, were likely to foster success in supply-chain continuity management.

They were:

- Risk awareness among top managers; this reflects the need to garner support within the business for necessary organisational changes and the implementation of supply-chain risk management measures
- An understanding that changes in business strategy change supply-chain risk profiles; the implications of such a change should be followed through with appropriate alterations made in continuity planning
- Risk management is an integrated part of supply-chain management; it should not be left as a bolt-on extra, or deemed to be the province of an isolated specialist risk department
- Each individual employee in each entity must have: a) risk awareness; b) an understanding of his or her role in the risk management processes

Moving on to the second 'P', 'Principles' are more explicit than philosophical issues, although they should still be few in number and wide-ranging across strategic and tactical levels of an organisation. Examples of principles that feature in risk management are failsafe design and duplication of capacity.

It is necessary to understand the principles employed by an organisation in order to reach a view on the effectiveness of their risk management and business continuity planning. The generic principles put forward in this research echo some of the primary tenets of current best practice in everyday supply-chain management, whilst drawing on the situation-specific risk elements.

Determining the appropriate practices to manage the supply-chain vulnerability issue in a particular situation appears to be context specific, dependent on, amongst other things, the supply-chain's response to the need for operational excellence.

However, this research concluded that the following generic principles apply:

- Risk considerations should influence the supply-chain design and structure
- Risk management should be based on a high level of supply-chain visibility and understanding amongst all entities
- Risk management should be based on clear performance requirements and lines of communication between all entities
- Supply-chain risk management should be based on process alignment and co-operation within and between the entities

The third 'P', 'Processes', embraces the processes, techniques and tools needed to manage supply-chain risk. This research acknowledges that there are a host of existing techniques and tools that can be employed to manage risk and plan business continuity. Not least amongst these are the 60 or so 'common' tools in the TQM toolbox.

At a tactical level, a set of activities should be carried out to prepare for and handle disruptions. These activities form the processes.

- Risk identification process – product/supplier/supply-chain related
- Risk assessment process – likelihood vs impact vs cost
- Supply-chain continuity management and co-ordination processes
- Processes to ensure learning from experiences

The pilot study research proposes that supply-chain continuity management should be approached in a systemic and holistic manner. The report suggests that a general approach to supply-chain continuity management is likely to proceed in a step-by-step approach, similar in many ways to the



## RESEARCH

approach taken in other general quality improvement programmes. The precise composition of the final toolkit will be the subject of further research. However, such a toolkit will reside within the context of the philosophical beliefs that guide behaviour in an organisation and an understanding of supply-chain management principles. These issues, in turn, set the context for employing a general approach to managing supply-chain risk.

Failure to consider these '3-Ps' and develop the appropriate techniques and tools for managing supply-chain vulnerability is believed to be a significant barrier to successful implementation. Beyond that, however, the research suggests that there are clearly

identified conflicts of interest that are also likely to make implementation difficult. These aspects, too, need further consideration, if they are to be overcome. There are, of course, some 'planned' rather than 'accidental' disruptions that no amount of contingency planning will ever be able to eliminate completely. Disgruntled employees may well be in a position to use their intimate knowledge of the organisation to circumvent well laid plans, processes and procedures, while other determined 'disruptive agencies', whether terrorists or protestors, will also adapt their behaviour accordingly. Therefore, organisations, and the supply networks within which they lie, must be sufficiently agile to respond quickly to these disruptive forces, whatever their source or nature.



### About the Authors

Paul Chapman, Professor Martin Christopher FCIT FILT, Uta Jüttner, Helen Peck and Dr Richard Wilding MCIT MILT work in the Cranfield Centre for Logistics and Transportation (CCLT).

Further information about this project and other on-going research at CCLT,  
Web site: [www.cranfield.ac.uk/som/cclt](http://www.cranfield.ac.uk/som/cclt)

Copies of the full report on supply-chain vulnerability are available, priced £35.00.  
Contact: Tracy Brawn. Tel: 01234 751122. Email: [t.brawn@cranfield.ac.uk](mailto:t.brawn@cranfield.ac.uk)

---