

Introduction

Risk managers understand that the consequences of damage by an unexpected incident may be measured in more than simply financial terms. There are more ways, and potentially much more destructive ways, of a risk incident harming an organization and its people than the loss of assets, revenues and cash flows, or the financial cost of litigation. The most destructive of impacts from a risk incident can be to render the organization unable to deliver on current contracts and continue to meet its responsibilities to stakeholders. A risk incident can also destroy an organization's ability to manage and retain control, and remain legal and compliant.

The impact may enforce a period of time when the organization cannot remain an effective player in its 'market-place'. It does not take long for that displacement to destroy brand values and other confidences or for competitors to rush in and wreak long-term damage to the organization's customer base and other important stakeholder dependencies. Even when the organization is a monopoly or public service supplier, the way stakeholders and customers react to a real or perceived fall in service levels can turn a hiccup into a disaster.

The risk manager must therefore ensure that all of the operational dependencies and tools necessary for the organization's survival remain accessible quickly enough to be of use. These dependencies are much more than money and assets. They include, crucially, a wide range of intellectual assets, effective business controls, regulatory approvals, legality, regulatory compliance, the confidence of its various stakeholders, its brand values and its reputation. It includes of course whatever assets, tools and skills – wherever they are positioned in the value chain – an organization needs to be able to continue to deliver urgent, contracted products and services, on time and of the expected quality. Extreme financial damage from an unpleasant surprise may indeed be sufficient to divert the financial business model sufficiently to render the organization no longer viable. The non-financial impacts, however, are equally, if not more likely, to bring greater damage or even corporate death.

The cause of that corporate death may be a sudden accident or indeed be a gradually evolving disease. The end result is the same and both are of equal

concern to the most senior management, its risk advisers and of course its stakeholders. A gradually developing disease, for example, a supplier's quality problems beginning to affect the brand value, is no less destructive and can be more difficult to manage than a sudden loss. It raises difficult questions of reaction timing, not least the judgement between a hope that the problems can be resolved and a decision that the plug be pulled immediately and the disaster reaction plan, with its own costs and challenges, be triggered.

Within earlier business models, the organization managed most, if not all, aspects of its supply chain from within its own factory, office, warehouse and workforce. It had more than one way of interfacing with its consumers, and maintained stocks of finished goods and raw materials on site to keep it going for days or weeks in the event of a failure or slow down in supply. It employed the workforce directly and thus had day-by-day control over each one of the activities that were part of the final delivery of its product or service. It could also instantly redirect that workforce to meet any new urgencies that had emerged suddenly through an unexpected incident or need.

The model enables inventories (with their expensive capital) management as security demand to be kept to an absolute minimum, often just enough for a few hours' productivity. It also enables the production levels and timing to match precisely with known demand or even pre-booked orders. It therefore dramatically reduces the dependency on accurate statistical forecasting of future demands that can only be based on past experiences and is always subject to variances and external risk influences. In this way, therefore, it can be used as a risk management value, not a risk management threat.

The modern business model, with its just-in-time supply chain, tight compression of margins, direct communication via the web simultaneously to millions of customers at home and abroad, is, however, much more brittle and has never been more susceptible to one single point of catastrophic failure. Furthermore, much of its workforce is now employed by a third party to deliver both intellect and activity, and only and precisely as agreed in a contract that had been negotiated at a time when the incident may not have been anticipated.

Outsourcing is no longer bolt-on for business, but an everyday way of life, at the local, regional, national and global levels. It is a way for businesses to focus on their core strengths and utilize the expertise of others to carry out the functions that the business is not as well equipped to perform. It is well named as a value chain: a name that illustrates that anything that happens in the chain of activities, from raw ingredient to final customer delivery, is designed to add value to that final product or service. If anything does not

add value or enables further value to be added, the activity is simply a cost drain and will surely be removed sooner or later.

Customers can move away so much faster – perhaps with just a click of the mouse – as indeed can competitors, upscaling quickly to steal customers. No longer do aggressive competitors, with the same business models available to them, need to raise capital, design and construct factories or office blocks and then recruit staff before they can upscale and attack a weakened organization. They simply sign a few new outsourcing contracts, maybe even with the damaged organization's erstwhile suppliers.

Vodafone reports that it does not actually manufacture anything. In 2006/07, it spent more than £20 billion on purchasing products and services from third-party manufacturers which themselves source components and assembled products from other suppliers.

These models enable the organization itself to upscale and downsize much easier and more quickly than before and thus offers opportunities to spread risk and manage a crisis. A diverse supply chain can therefore be a useful risk-spreading tool as well as, when not effectively risk managed, a way of concentrating risk into single, potentially catastrophic, failure points.

The increasing importance of this wider potential for damage now lies at the very core of business models. It takes the risk manager and the most senior strategic managers of the organization way beyond the range of their financial risk management comfort zones, where, over many years, they have developed sophisticated financial risk models. It takes them into the much more amorphous and difficult arena of operational risk, particularly into areas of very low-frequency but very high-impact risks. It needs them to understand and respond to the fact that they are simultaneously shedding the ability to micro-control, shedding the very tools that they need, whilst exposing themselves to second-hand risks, impacts and frequencies much more difficult to evaluate, communicate and manage.

Throughout this book, the expression 'risk manager' does not just extend to those professionals who may carry this title. Generally speaking it will apply to those persons who have the responsibility to accept risk and/or give advice to senior managers that will place them in a position where they can make more informed, and therefore better, decisions about risk, impact, risk tolerances and risk management. This risk viewpoint can be from any director or manager who needs to address risks, and may come from a wide range of quite different risk-related titles across the organization.

Managing Risk and Resilience in the Supply Chain

Risk management has moved on from being simply the purchase of insurance products. Business continuity management is emerging from its own historical silo of technology and workstation replacement. Regulators are increasingly pulling operational risk concerns into compliance management, and even credit risk management should not fail to consider operational risks that could take away a debtor's ability to pay, nor indeed the single points of infrastructure failure that could affect separate debtors simultaneously. The realities of modern business models and their risks therefore cut right across these and the other silos of risk management that were, on the whole, previously able to deliver their values in isolation.

Risk exposures now have common roots and causes right across the whole spectrum of risk and strategic management frameworks. Of course risk management is as always as much about risk taking, and thus about opportunity, as it is about damage. Effective management of today's organizations therefore is not just about taking time out occasionally to consider risks, nor to search out ways that they can tick regulators' boxes. It is, quite simply, about good management, and, increasingly, survival. It enables the investment in activities and resources to be measured properly, and not only by the management itself but also by the organization's own stakeholders. Clearly a high return on a risky investment is just not the same value as a high return on a less risky one, a fundamental principle of business from time immemorial. The investor clearly wants a higher return if a higher risk is being carried, and above all, the investors of money, time, resources or reputation, need to be able to understand and measure the risks they are carrying.

Risk management is no less an enabler, when otherwise profitable opportunities are avoided because of an anecdotal fear of the risks that they may carry.

The outsourced value chain is clearly at the very heart of the resilience of modern day organizations, whether they are profit-making, public service or indeed charity. It brings real challenges in gaining an understanding of what those risks are, and indeed it brings a whole new range of risks and potential impact. The outsourced value chain also reduces or removes the manager's ability to micro-manage. It cannot hand over the responsibility for risk to third parties, but conversely it must delegate the management of some important risks to people whose relationship is only as defined within a precisely worded legal document.

These people must always put the interests of their own organization first as they are charged to do so by their own employers and stakeholders. The risks placed in their hands can be potentially lethal and include, not

least, the day-to-day ownership and management of crucial dependencies such as intellectual assets, the ability to deliver, legality, reputation, quality, compliance, the availability of workforces and their skills and experience.

This book sees the ‘supplier’ as a potentially crucial and urgent dependency. It sees the receiver as a dependency too of the ‘supplier’, which can be damaged or destroyed by the failure of the recipient’s ability to receive the goods or services as contracted, or to retain the supplier’s confidence that they are going to get paid for them. It sees the organizations further up the value chain delivering the organization’s products and services equally as ‘suppliers’ of these distribution services to the organization. The book sets out to explore the ways that supply chains can go wrong, either suddenly or gradually, and to discuss the strategic risk understanding and management of supply chains that are at the very heart of the effectiveness of modern day management.

This book therefore will explore these business models and in particular the dependency management that has become such a crucial management need, embracing not only infrastructures but also the other equally important corporate life support systems that we have listed.

Above all the book recognizes that outsourcing is so much more than sub-contracting an individual task or the manufacture of items for the production line. It is about the strategic positioning of core elements of the organization and its dependencies into the hands of third parties.

Some outsourcing contracts are huge: in 2005 there were 11 deals valued at over US\$1 billion. In a FM Global survey in 2006, ‘supply chain’ topped the list of risks causing major disruption. A survey by AON lists ‘loss of reputation’ and ‘business interruption’ as key concerns, both of which are supply chain dependencies. An interesting case study to set the scene is The Association of Clearing Houses.

The Association has three main constituent companies: Cheque and Credit Clearing Company Limited (bulk paper clearances); CHAPS Clearing Company Limited (same day electronic clearing); and BACS Ltd (bulk electronic clearing).

CHAPS provides core services to 29 banks and financial institutions clearing on average £200 billion a day. This is just part of the picture. BACS, the automated clearing house, handles 14 million electronic debits and credits a day, averaging £9 billion. A high peak day would see 57 million transactions and 80 per cent of UK adults are paid through the BACS system. In addition, the company handles cheque and credit clearing, debit and credit card transactions and processing, and ATM and cash transactions.

Moves to real time settlement have increased single points of risk to exposure that would simultaneously damage or delay these millions of financial transactions and perhaps even the country's economy. Just one of the lessons addressed after the September 2001 debrief was that, whilst there is diversity of backup data, there may not always be diversity of control systems and indeed it is likely that some routings previously perceived to be diverse, actually converge.

The widespread and simultaneous impact of damage by such a service supplier organization could destroy its customers' own continuity plans. Whilst risk activity can be delegated, the responsibility for risk cannot. Dependence on such organizations therefore demands that the recipient organization itself ensures that those exposures are controlled and can illustrate that risk control to its customers and regulators.

In summary, the responsibilities and demands of the strategic management of an organization do not change when a part of the core activity is repositioned with a third party. Understanding and retaining control over the risks of those activities, and retaining at the same time the freedom to fully exploit their commercial value, does however bring very different problems, balancing acts and challenges.

David Kaye

FCII FBCI FRSA MIRM

Davidjkaye@aol.com

Risk management and modern day business models

Impact vs risk

A risk manager will routinely consider not only the risk of something happening that could divert the organization from its objectives and responsibilities, but also the likelihood and/or possible frequency of such an incident. Equally important to the risk manager is precisely how the likely impact of that incident could damage the individual sensitivities of the organization and its people. Understanding that impact entails a strategic understanding of the commercial activities of an organization, its role within its market-place, its differentiated positioning from whatever competitors it has, and its sensitivities to holding that positioning.

It also entails understanding what makes the organization tick and the wide range of hard and intellectual dependencies that are keeping that organization in its position. Each organization will have its own individual sensitivities, just two of which will be the ability to remain legal, and to continue to deliver to its own range of stakeholders all of the expectations that have emerged 'in the good times'.

As part of the risk policy statement, the risk manager will have defined graded levels of impact for 'risk-taking colleagues', i.e. all those responsible for a division or support function. This will not only include financial cost; indeed one challenge is to grade financial and non-financial risk in a consistent way. It will include the impact of the organization's inability to deliver on its promises to stakeholders and becoming weaker within its market-place. This will naturally embrace those things that are crucial to that ability to deliver as promised. As a consequence, the element of 'maximum possible time out' is one of the crucial assessment criteria and this will vary from organization to organization and by type of business.