UNIVERSITY OF AUCKLAND Business Review
Volume 8 No. 2

Managing the new global threats

By Peter Enderwick

Managing the New Global Threats

By Peter Enderwick

Focusing on strategy rather than traditional risk management may be the best approach to managing threats in the new global business environment.

GABRIELLE HOPE, *Untitled*, watercolour on paper (540 x 365mm)
The University of Auckland Collection

The emergence of new global business environment threats – terrorism, global diseases, computer viruses – raise major challenges for the management of international business. These global threats are characterised as "jolts" which occur randomly, they "evolve" changing their nature, and their impact tends to be concentrated by sector or geographical location. They are more accurately considered as uncertainties rather than risks.

This paper suggests that the most effective approaches to managing these threats focus more on firm strategy than on traditional risk management. The key strategic responses are likely to occur in the areas of supply chain management, diversification, scenario planning and ensuring business continuity and the principal management implications for these areas are discussed.

Introduction

The business environment is characterised by major threats and opportunities. Both threats and opportunities are particularly significant for organisations operating internationally. The nature of their operations means that they cross cultures and geopolitical fissures. While it is the potential opportunities that encourage internationalisation, the accompanying threats have to be managed.

Environmental threats can have a devastating impact on any business. Statistically, a large company can expect a crisis once every four to five years, and the costs they face can be fatal.[1] Crisis Management International suggests that of businesses facing a disruption of at least 10 days, 73 % close, or suffer long-term damage.

Some 43 % of businesses suffering a disaster never recover sufficiently to resume business, and of those that do reopen, less than one-third survive for two years or more. These costs apply to all business; indeed the financial losses suffered by small firms tend to be proportionately greater than those of larger firms.[2]

All businesses are likely to be victims of the new global environmental threats such as terrorism, computer viruses and global disease that have become a major concern in the last few years. Business has long been a favoured target of terrorist attacks. Since 1968, when the U.S. government began to monitor terrorist attacks, 80 % of attacks on U.S. interests have been against businesses.[3] Computer viruses impose major costs on business operations. The reality is that these threats must be understood and managed. In part, the challenges that arise are a result of the relative infrequency of these events, their evolutionary nature, and the fact that many of the costs stem not from the events themselves, but from subsequent government policy responses. This is certainly the case with international terrorism where new security policies have imposed huge additional costs on shippers and carriers.

The intention of this paper is to examine these new global threats, to distinguish their precise nature, and to develop their implications for risk management. The paper is organised into five substantive sections. The following section provides background on the evolution of the international business environment and the changing nature of strategy formulation. Section three analyses the nature of the new global threats suggesting that these constitute uncertainties not risk. The strategic implications of these threats and how they are best managed is discussed in section four. Some implications for New Zealand business are discussed in section five. The final section provides concluding thoughts.

Evolution of the global business environment

Changes in international business in the past few decades have brought greater internationalisation and integration. These changes are commonly captured in the term "globalisation", which manifests itself as increased cross-border movements of goods and services, capital, technology and people. Growing internationalisation and integration have been facilitated by declining trade and investment barriers, the growth of free trade agreements and regional integration, as well as technological advances in communications and transport.

Globalisation has provided significant opportunities for firms to reconfigure their supply chains and globalise production systems, thereby reaping economies of scale and taking advantage of national differences in factor cost and quality. While globalisation undoubtedly brings considerable cost savings it also presents some significant challenges. The interconnectedness that is characteristic of globalisation means that local conditions are no longer simply the result of purely local influences. Similarly, the impact of seemingly localised events can spread rapidly to become regional or global problems. This was certainly the case with respect to the Asian Economic Crisis and the SARS virus.

At the same time structural change in the international business environment has increased vulnerability to threats. The scale of investments in today's globalised world, coupled with rapid technological change, a shortening of product life cycles and the increasing aggressiveness of competitors,[4] have increased the uncertainty and complexity of operating globally.

Unlike earlier decades that exhibited long, stable periods in which firms could achieve sustainable competitive advantage, competition is increasingly characterised by short periods of advantage, marked by frequent disruptions.[5] In such "hypercompetitive" environments, threats are not so much predicted as they are responded too. Accordingly, strategies which focus only on efficiency and cost structures are now being reassessed in light of the inflexibilities they exude in a changing and uncertain environment. Further, exploitation of core competencies that were once seen as a precondition for success, are increasingly seen as presenting the risk of core rigidities.

Changing perceptions of business strategy

The changing nature of the business environment has cast considerable doubt on traditional approaches to strategy formulation. Greater volatility of the environment has occurred over a number of years manifested as increased product introductions, the creation of new industries and the blurring of boundaries between established sectors, declining corporation life-spans, widespread regulatory changes, and increased technological connectivity.

Traditional strategy approaches are based on the assumption that the past is an effective guide to the future. Indeed, assessment of the relevant probabilities even allows the generation of a single point forecast. However, volatility has now become so commonplace that it is increasingly accepted as the "new normal"[6] and the view of strategy is shifting away from steady state concepts such as vision, mission, and core businesses.

Increasingly, effective organisations seem to emphasise process and dynamics, even at the expense of analysis. This is not to suggest that intuition is an effective substitute for analysis. Indeed, in a highly volatile

Peter Enderwick is Professor of International Business at Auckland University of Technology.

environment it is unlikely that managers will have had previous experience of such conditions and the usefulness of intuition is obviously limited. Emerging environmental conditions emphasise flexibility and experimentation and a degree of non-alignment between the organisation and its environment. This has resulted in a number of new approaches to strategy determination including the "portfolio of initiatives approach",[7] strategic innovation,[8] and strategy as simple rules.[9]

Traditional conceptions of risk

In the same way that traditional approaches to strategy are being reconsidered, the same can be said of risk management. Until the mid-1990s "risk" was generally equated to financial, inflationary and political risk, largely specific to the host country. Political risk was country-specific and could be summed up as the likelihood that an Multinational Enterprise's (MNE) foreign operations could be constrained by host government policies through measures such as forced divestment, unwelcome regulation, and interference with operations. Accordingly, risk-management was also country-specific, and involved assessing the riskiness of a particular country through a variety of predictive approaches. Other risk-management devices also involved responding to risk emanating from host governments. Defensive political risk management strategies implied locating crucial aspects of the company's operations beyond the reach of the host, while integrative strategies aimed to make the firm an integral part of the host society, thereby reducing the likelihood of detrimental government interventions.

However, as the world economy has become increasingly global, political risk, while still present, is arguably not as pressing as before. This is largely because of changing attitudes towards trade and investment, with most countries now encouraging foreign direct investment (FDI). Indeed, between 1991 and 2003, more than 165 countries made 1885 changes in legislation governing FDI, with 95 % of these changes involving the liberalisation of FDI regulations. This has also been supported by a dramatic increase in the number of bilateral investment treaties, as well as regional and global free-trade agreements.[10]

Recent years have witnessed the emergence of a new type of business threat that has manifested itself in incidents such as global terrorism, SARS, financial crises, and computer viruses, all of which have the ability to disrupt a firm's operations. Such threats are sudden, unexpected and unpredictable with a tendency to spread quickly through global processes and forces, thus having a widespread impact, but with a disproportionate impact on regions, sectors and industries. Clearly, risk is no longer country-specific, nor is it limited to threats from host government actions. Instead, it is global and systemic, and capable of being perpetrated by individuals or small groups. Further, such threats do not simply affect a firm's operating conditions, but also its overall viability, as they can cause severe disruptions threatening the very survival of the firm. It is not easy, and in some cases not possible, to insure against such risks. Following 9/11 many companies found that their insurance coverage became prohibitively expensive or was discontinued. For example, Delta Airlines terrorism insurance premiums increased from $2 million in 2001 to $152 million in 2002.[11] As long as the insurance industry remains wedded to actuarial approaches to risk assessment, and until sufficient data exist to allow appropriate calculations, coverage is unlikely to be available.

Accordingly, new strategies for managing this type of threat are required, and such threats cannot be avoided by simply deciding not to invest in a particular country, or by using strategies centred on host governments. However, while in the past risk was largely seen as negative, it should be noted that these environmental uncertainties provide both challenges and opportunities for those businesses that are able to respond quickly and effectively.[12]

Nature of the new global threats

It is useful to clarify the exact nature of these threats in terms of risk and uncertainty. While these terms are often used interchangeably, they have distinct meanings.[13] Since Knight's analysis, risk is considered as the variation in potential outcomes to which an associated probability can be assigned. In statistical terms, while the distribution of the variable is known, the particular value which will be realised is not. Uncertainty exists when there is no understanding of even the distribution of the variable. For decision-making, uncertainty is a greater problem than risk. Because probabilities can be attached to risk, options to mitigate risks through insurance or hedging are possible. Because probability cannot be assigned to uncertainty, instruments to reduce uncertainty are not available.

This discussion suggests that new global threats such as SARS, avian bird flu, global terrorism and computer viruses are uncertainties, not risks. These types of disruptions share a number of characteristics. First, they can be considered as "jolts"[14] which occur randomly. Because such events are not continuous or even regular, it is not possible to assign probabilities to them. Second, the nature of these jolts is such that they "evolve", changing their forms; they do not simply recur. For example, viruses such as SARS and avian bird flu are capable of mutating and assuming different forms with differing impacts. In the case of avian bird flu there have been recent reports of the first full case of human-to-human transmission and a recurring fear is that it could mutate into a human pandemic with devastating effects. Similarly, global terrorism assumes a

variety of forms including car bombs, suicide bombers, aircraft as weapons of destruction, and chemical attacks. This makes it difficult to use historical experience as a predictor of future occurrences and impacts. Third, the impact of these uncertainties tends to be concentrated, either by sector or by geographical location. For example, the primary effects of SARS were experienced in Asia and disproportionately affected the transport, tourism and medical industries. The impacts of natural disasters such as extreme weather events, or financial and political problems, appear to be more widely and randomly distributed.

The threat and cost of these disruptions are considerable. More businesses seem to be prone to security breaches and computer viruses, and attack-related downtime has increased.[15] Recent surveys suggest that while few businesses expect to be the victim of a terrorist attack, they do rate security as a top priority and it is seen by many as an issue of growing significance.[16] The worldwide cost of computer viruses and worms was put at $12.5 billion in 2003[17] and the number of attacks has increased dramatically in the last decade.[18] A significant number of companies now recognise considerable vulnerabilities in their supply chains.[19]

As well as the direct costs of these events, they are also associated with sizeable secondary costs as governments intervene to try to eliminate or reduce the likelihood of global threats. The secondary costs stemming from new policies are often considerable. The maritime industry is likely to face extra costs of $8 billion per year over the next ten years, the trucking industry almost $100 million a year, and airlines an extra $315 million a year.[20]

For businesses the costs of recovery from a significant disruption are also considerable. These costs include loss of revenue, shareholder value, and customers, as well as deterioration of brand equity and reputation. Table 1 provides a summary comparison of traditional and emerging risks.

Strategic implications

The above discussion on these new global threats suggests that they are both new and novel and this has important implications for the way uncertainty is managed. Risk management strategies that were largely country-focused are no longer adequate in themselves, given that this new type of threat is global and systemic. Furthermore, businesses cannot assume that the management of global threats can be delegated to their governments. First, in an interdependent global economy governments have limited ability to deal with these problems. Their solution requires a concerted effort from both the public and private sectors. Second, government policy responses to these threats add to the challenges that firms face. For example, the policy response to 9/11 has added considerably to the costs of international commerce as well as the ease with which funds and employees can be transferred. This is part of the ripple impact of these new global threats.[21]

It is also important to distinguish between security and resilience within a system. Security refers to the ability to maintain the integrity of a system, while resilience is concerned with the ability to react and respond to a disruption. While the two characteristics are seen as desirable, they may be incompatible. For example, while moving to multiple sources of supply may increase resilience through continuity of supply, it is likely to increase the difficulty of achieving security.[22]

Despite the high levels of uncertainty associated with these events, this should be incorporated into decision-making. There are four broad approaches to dealing with uncertainty. These are i) to predict, to try to obtain more information on the phenomenon; ii) to balance or mitigate uncertainties perhaps through diversification; iii) to try to control or influence events; and iv) to increase flexibility and responsiveness. It is unlikely that individual businesses can use option iii) and try to control these

Table 1: A Comparison of Traditional and Emerging Risks

	Traditional Risks	Emerging Risks
Examples	Single issues e.g. foreign exchange risk, political risk	Systemic nature e.g. SARS, terrorism, Avian bird flu
Characteristic	• Recurrent • Probalistic • Largely unchanging • Broad impacts	• Novel • Non-probalistic • Evolutionary • Specific impacts
Response Strategies	• Risk prediction • Risk forecasting • Country-specific management focus • Government as a major source of risk • Risk primarily negative • Risk impacts primarily on operations • Focus on risk containment and management • Individual responses	• Risk response • Risk modelling e.g. scenario planning • Systemic risk management focus • Individuals, groups and localities as major sources of risk. Government role in responding to risks • Risk both negative and positive • Risk can threaten viability • Focus on strategic responses and management • Collective responses

environmental threats. Most business responses have focused on the other three.

A lack of precise knowledge about a particular event does not preclude decision-makers from further information gathering or from making decisions about likely probabilities of events occurring. As has been recognised, traditional strategic management approaches encourage perceptions of uncertainty in a binary fashion.[23] The world is seen either as sufficiently certain that precise, and usually single, predictions of the future can be made, or that uncertainty renders such an approach totally ineffective. In the latter case there may be a temptation to abandon analytical approaches and to rely wholly on gut instinct. Courtney et. al.[24] argue that in many cases uncertainty can be significantly reduced through careful search for additional information, in effect much that is unknown can be made knowable. The uncertainty that remains after the most thorough analysis they term "residual uncertainty".

There are a number of approaches which offer insights into how to manage residual uncertainty. The simplest approach is to ignore it. This can be done by developing a "most likely prediction" often based on "expert input" or by assigning a margin of error to key variables. Each of these approaches yields a single unequivocal strategic option by either ignoring uncertainty or assigning it a probability. Neither approach is satisfactory. Ignoring an uncertain environmental event is clearly dangerous. Assigning probabilities to unique events is invalid. Even subjective probability derived from expert analysis is untestable and arbitrary.

Miller[25] highlights a useful distinction between financial risk management and firm strategy approaches to managing environmental uncertainties. Financial risk management techniques such as insurance and futures contracts reduce the firm's exposure to specific risks without changing the underlying strategy. But, as noted above, such techniques only apply to risks, not uncertainties. In the case of an event such as global terrorism or SARS, strategic responses which attempt to mitigate the firm's exposure to uncertainties are likely to be more useful. Miller[26] identifies five generic strategic responses to environmental uncertainties: avoidance, control, cooperation, imitation and flexibility.

Avoiding this type of event through divestment, delayed entry or a focus on low uncertainty markets is difficult. The irregular occurrence and variable impact of such events is unlikely to justify divestment. Similarly, their unpredictable and evolving nature makes postponement or niching very difficult. Uncertainty control strategies based on political lobbying, vertical integration or enhanced market power are not an effective counter to most of these new uncertainties. In the same way, a cooperative strategy deals primarily with behavioural risk and is not likely to be effective, neither is an imitative strategy which addresses competitive rivalry. Of more value is the management of uncertainty through organisational flexibility. Flexibility focuses on the ability of the organisation to respond and adapt to significant environmental changes. High levels of flexibility imply lower costs of organisational adaptation to uncertainty.

In contrast to approaches which try to increase the predictability of uncertain events, flexibility strategies emphasise internal responsiveness, irrespective of the predictability of contingencies. However, the benefits of flexibility can easily be oversold. Larger organisations achieve competitive advantage through investment and commitment. Such commitment and appropriate investments assume good understanding of the future. Since forecasts of the future are always imprecise, there may be temptation to delay investments in the development of new capabilities and markets in an attempt to retain "flexibility". The result is likely to be a loss of competitiveness. A refinement on the need for flexibility is the more structured alternative of scenario planning tied into real options (see below).

A widely used strategy for increasing flexibility is diversification, whether of products, markets or sources of supply. With regard to the contemporary global threats discussed above, the key strategic responses are likely to occur in the areas of supply chain management, diversification, scenario planning and ensuring business continuity. We consider these in more detail.

Supply chain management

Supply chain disruptions are not new. The September 21, 1999 earthquake which hit Taiwan curtailed the supply of computer chips adversely affecting HP, Dell and Compaq. In 1996 GM had to temporarily layoff 177,000 workers at 26 assembly plants as a result of an 18-day strike at two brake manufacturing factories.[27] The move towards the elimination of waste in supply chains has brought not only cost savings [as much as $150 billion a year][28] but has also exacerbated vulnerability. The ratio of stocks to shipments of U.S. manufactures fell from 1.62 in 1992 to 1.30 in the year 2000. Higher rates of new product introduction, longer, international supply lines, compressed lead times, a preference for single sourcing, and lean inventories have all heightened vulnerability and increased the complexity of supply chains.

The new threats are bringing significant changes in the management of supply chains.[29] There is evidence of a preference for secure, long-term supply relationships. At the same time many companies are reconsidering the benefits of overseas suppliers which, while offering lower cost sources, are often susceptible to costly disruptions.

As the advantages of lean production and supply chains are being reconsidered, a variety of solutions are emerging. One argument is to move from sole to multiple sourcing within the supply chain. This can be achieved

in a number of ways, including local secondary sourcing, reserving capacity within other supply sources, and using a supplier with multiple locations.[30] A variant of this is dual sourcing with preferred overseas suppliers being responsible for the majority of supplies, but a fraction of the business going to a local "shadow" supplier. Considerable investments in backing up processes and knowledge are also occurring. Back-up is more than simply dual data banks. More generally, knowledge can be backed-up through the documentation of critical processes, increased cross-training and standardisation of processes and practices across the enterprise.

There may be ways to improve the security of supply chains without losing the very considerable cost advantages developed in recent years. Lee and Wolfe[31] argue that the lessons of total quality management (that higher quality can mean lower costs) are pertinent. To date most of the initiatives have focused on improved information flows and risk pooling. Closer coordination and the sharing of information along the supply chain help to reduce the likelihood of stock-outs and "bullwhip effects". Such coordination is much easier with new inter-enterprise computer standards. Risk pooling is possible because forecasts of more aggregate phenomena are more accurate than disaggregated ones. To take advantage of this, firms can use strategies such as reducing product variability, mass produce modular designs and adapt products close to the point of sale, build to order, or centralise inventory.[32]

One complication in the effective management of supply chains is the recognition that the greatest disruption and damage arises not simply from the threat, but from government policy responses to these events.[33] This was certainly the case with 9/11 where governments closed borders, halted air-traffic, and froze financial transactions. It is enhanced security measures that have raised costs and increased delays in international supply chain systems.

Diversification

Diversification of products, markets and processes is a well-established technique for managing risk. However, such risk management may be at the expense of returns. While the strategic management literature has emphasised the likelihood of excessive product diversification lowering returns,[34] there is evidence that at least modest diversification may be positively related to business performance.[35] Geographic diversification also exposes the firm to the problems of political and cultural risk.

The move in recent years towards the outsourcing of business processes may have helped to reduce costs but care should be given to risk assessment of such activities. Dependence on politically volatile areas and the integration of complex global supply chains can be managed but it requires the careful balancing of three aspects of the offshoring decision: geography, the stage of value-added, and the type of activity outsourced.

The strategy of diversification and, in particular, the form that diversification assumes, has also been affected by the emergence of the new global threats. Diversification through international acquisition raises not just operational and cultural challenges but also exposes the company to direct attack. Achieving a similar level of diversification through strategic alliances may offer greater resilience, but also increases interdependence risk.[36]

Scenario planning

High rates of change and the resulting uncertainty do not mean that planning is no less important, but it does mean that the form of planning may change. A number of organisations have begun to experiment with approaches such as scenario planning.[37] Scenario planning is a useful technique for considering the long-term future.[38] It is most appropriate in situations that involve high levels of uncontrollable, irreducible uncertainty. It is based on the idea that many different futures are possible, each of which is contingent upon the evolution of a variety of factors.

It is useful to contrast forecasting and scenario planning. Forecasting is based on an assumption that past and present conditions provide a good indication of the future. They therefore assume a high level of structural inertia. In the very short term forecasts are likely to provide little more than trivial insights; in the long term residual uncertainty is likely to render them meaningless. In contrast, scenarios are descriptions of possible future outcomes and not a prediction of a particular outcome. Because uncertainty increases with the time-span of the decision-making horizon, scenario planning is most useful in assisting long term decisions.

Scenario planning approaches offer a number of advantages. The principal advantage is that by forcing an organisation to consider a range of possible futures and the factors likely to shape these, it increases flexibility and resilience in the face of uncertainty. The organisation no longer simply reacts to a changing environment. Scenario planning also enables the pooling of qualitative and quantitative information which in combination should improve the quality of decision-making. It can also be used to integrate social, bio-physical, political, economic and technological factors. Furthermore, the participative nature of scenario planning assists in the building of shared understanding. Since distinct futures have to be reconciled with the capabilities and investments of the organisation, scenario planning encourages learning and adaptation. It can be a powerful mechanism for instilling a culture of learning.

However, there are several weaknesses. One is the

possibility that the scenarios generated blind the organisation to other possible outcomes. There is also the danger that the scenario planning process simply creates a "knowledgeable elite" of those directly involved and that future views are not effectively diffused and shared. In some cases scenarios are too simplistic, perhaps portraying just optimistic and pessimistic alternatives.

More recent analyses have tied the scenario planning approach to real options thinking. Such analyses highlight the importance of matching future scenarios to the development of appropriate skills and knowledge to ensure effective strategic execution. While investments in future capabilities which are known with a high degree of certainty are likely to be undertaken, the same cannot be said of contingent elements. Here the firm may choose to exercise "real options" over contingencies. Real options are a means of hedging strategic risk.

A real option gives an organisation the right, but not the obligation, to increase investment or control over a contingent element supportive of a particular scenario.[39] Potentially useful assets can be locked up in a variety of ways which enable progression towards full or controlling ownership. Common methods include alliances, licensing agreements, and joint ventures with the possibility of subsequent partner buy-out.

Over time, as uncertainties become resolved, the firm will exercise some options, abandoning others. Options are particularly attractive with projects that are reversible or divisible. In such cases, delays, modifications, or fragmentation of projects can facilitate both learning and the clarification of uncertainty. The relationship between scenario planning and real options is a two-way one. For example, scenarios can be useful in foreseeing, evaluating and the timing of real options.

Business continuity

The pervasive nature of the new global threats has encouraged a shift in management thinking away from simply responding to a single event or occurrence towards a focus on ensuring the continuation of operations. This is the field of business continuity which is concerned with ensuring that a business can continue to operate even in the face of powerful threats. The key to successful business continuity management is an understanding of the mission critical processes within the organisation. Particular vulnerabilities are likely to be found in supply and customer relationships, manufacturing and assembly processes, as well as information systems.

Traditional approaches to business continuity which focus on the impact of a natural or man-made disaster at a single site offer little protection against the emerging global threats considered here. Firms need to move beyond responding to single events to preparing for any eventuality. Furthermore, current thinking is moving beyond a focus on minimising recovery time from a crisis

to ensuring that operations, or at least critical activities, can be assured.[40]

An aspect of increasing importance to business continuity is the changing relationship between information and goods flows. Increasing separation and the extension beyond the immediate enterprise of these two streams in the value-chain mean that particular attention must be given to protecting information assets. In the global era where alliances and offshoring arrangements are widespread this may mean extending business continuity capabilities to partner organisations. There is considerable evidence that firms focus on internal risks rather than on network or supply chain risks.[41]

Implications for New Zealand

Our discussion has a number of implications for New Zealand business. The structure of the New Zealand economy puts it in a unique position. On the one hand, New Zealand's hazard prone location (situated on major fault line) and dependence on agriculture make it vulnerable to natural and biosecurity threats. At the same time, recognition of such vulnerability has created widespread awareness, a high level of border security, and experience in dealing with pests such as the Painted Apple Moth. A second feature of New Zealand is the small average size of organisations, possibly limiting the amount of time and resources that are committed to threat detection and management. This suggests that New Zealand business may place considerable reliance on government organisations to provide leadership in the event of a major threat. A corollary of this is that New Zealand businesses may not be well prepared for handling a significant low probability, high consequence event.

Direct evidence on these questions is very limited. Indirectly, we do know that the New Zealand authorities have committed considerable resources to minimising the risk and impact of natural and biosecurity threats. Similarly, the lead organisations have significant experience in handling significant events including flooding, the Foot and Mouth scare on Waiheke Island, and Auckland's major power failure in 1998. However, there has been some concern regarding the effectiveness of public sector responses to such events. Recent civil defence Tsunami exercises and the Operation Taurus simulation of an outbreak of foot and mouth disease revealed problems of cross-organisational coordination and communication difficulties.[42] More generally, they raise important questions concerning the amount and type of training that is required in responding to low probability, high impact events. For businesses this is an important commercial decision; studies reveal that business disruption costs generally far exceed property losses in this type of event.

Evidence on the relationship between firm size and ability to respond to business threats confirms that larger organisations appear to be better prepared and more likely to have crisis management teams[43] than smaller businesses.[44] Indeed, while the New Zealand Ministry of Economic Development website provides an example of a Workplace Influenza Pandemic Healthplan, this is drawn from Shell Australia, a very large and well resourced organisation. Similarly, it is known that large organisations including Progressive Enterprises, Air NZ and Vodafone are the most advanced in planning for a possible avian flu epidemic. However, recent research suggests that even within large organisations the general level of preparedness appears to fall sharply after the occurrence of a particular event[45] and that few organisations actually conduct vulnerability audits.[46]

Changes in the structure and size of New Zealand organisations since the restructuring of the mid-1980s have also been linked to likely effectiveness of a crisis response. Brunsdon and Dalziell[47] suggest that the increasing independence and fragmentation of New Zealand organisations, particularly within the public sector, have created problems of a "silo mentality", fears that coordinated planning may be interpreted as collusion, a loss of strategic expertise, and the suppression of clear crisis leadership.

Conclusions

The changing nature of the international business environment brings new threats which must be effectively managed. Threats such as global terrorism, diseases and computer viruses mean that the effective management of risk and uncertainty is an increasingly important skill within international organisations. The new global operating environment raises many challenges. It throws into doubt the traditional focus of many business operations, including repeatability versus unpredictability, market versus preferred supply relations, and collaboration versus secrecy.[48]

Many organisations are struggling to come to grips with these challenges. Traditional risk management options such as insurance or diversification are of limited value in the face of these threats. Simplistic responses to increasing uncertainty such as reliance on intuition are unlikely to be effective as uncertainty is usually the result of too much, or too little information. Rather, we argue that the appropriate response is likely to involve significant strategic and organisational change.

For a variety of reasons such change is difficult to instil. For example, there is growing concern that legislative and other changes in the West mean that managers are both less tolerant of, and less able to respond to, uncertainty. The fear is that the more risk is controlled and legislated the less able managers are likely to become in dealing with risk.[49]

Currently, security is seen as an additional cost or

burden on organisations and the focus is on how such costs are to be shared. However, in the medium term security may be seen as an investment and not simply a cost. For example, firms will need to invest resources to share information with government agencies and are likely to assume some of the additional security costs. However, this may provide a pay-off where, for example, a company obtains faster clearance through the use of certified or approved carriers and shippers throughout the supply chain. While New Zealand organisations are certainly vulnerable, we know very little about their preparedness. This is an area that would benefit from research.

In the long-term we may expect to see significant changes in the way in which environmental threats are perceived. Technologically, we might expect the development of "fail smart" technologies which enable systems to fail, but to capture and retain valuable information at the point of disruption. Modern information technology means that such systems are already possible. Attitudinally, uncertainties could become the new normalcy and strategic and structural adaptation effective in countering emerging threats. Major attitudinal changes will be necessary as an uncertainty culture becomes embedded in most international organisations and perhaps begins to converge with dynamic adaptive and learning processes.

References

1. Reiss, C. & Connolly J.M. (2003). *Crisis Management Leadership: Lessons Learned and Returns on Investment.* Unpublished paper, New York: Marsh and McLennan.
2. Singhal, V. & Hendricks, K. (2003). *The Weakest Link*. Paper presented at the 2003 Council of Logistics Management Conference, Chicago, Ill.
3. Rice, J.B. & Caniato F. (2003). *Supply Chain Response to Terrorism: Creating Resilient and Secure Supply Chains.* Supply Chain Response to Terrorism Project Interim Report, August, Boston: MIT Center for Transportation and Logistics.
4. Volberda, H. (1998). *Building the Flexible Firm.* Oxford: Oxford University Press.
5. Volberda, H. (1998). See endnote 4.
6. Accenture. (2003). *Executive Issues 2003: Is Uncertainty the New Normal?* Bermuda: Accenture.
7. Bryan, L. (2002). Just-in-time strategy for a turbulent world. *The McKinsey Quarterly 2002 Special Edition – Risk and Resilience,* 16-27.
8. Hamel, G. (2000). *Leading the Revolution.* Boston: Harvard Business School Press.
9. Eisenhardt, K.M. & Sull D.N. (2001). Strategy as Simple Rules. *Harvard Business Review.* 79(1), 107-116.
10. UNCTAD. (2004). *World Investment Report 2004: The Shift Towards Services* New York and Geneva:

UNCTAD.
11. Rice, J.B. & Caniato F. (2003). See endnote 3.
12. Enderwick, P. (2004). New Uncertainties Facing Strategic Planners, With Particular Reference to the Impact of Terrorism and SARS. *Strategy Magazine,* No 2 Jan, 14-16.
13. Knight, F.H. (1921). *Risk, Uncertainty and Profit.* Chicago: University of Chicago Press.
14. Meyer, A.D. (1982). Adapting to Environmental Jolts. Administrative Science *Quarterly,* 27, 515-537.
15. Hulme, G. V. (2004). Under attack [Electronic Version]. *Information Week*. Retrieved 26 July 2006 from www.informationweek.com/story/showArticle.jhtml?articleID=22103493
16. Claridge, D. & O'Brien K.A. (2004). *Terrorism and Business Continuity Survey 2004*. London: Janusian Security Risk Management, 9 May.; Evans, C. (2002). The State of Private Sector Security: A Year Out from 9/11. *Competitiveness Watch.* 1(3), 7 October. Washington: Council on Competitiveness.; Van Opstal, D (2003). Private Sector Stepping Up to the Plate on Security. *Competitiveness Watch. 2* (3), 5 November, Washington: Council on Competitiveness.
17. Hulme, G. V. (2004). See endnote 15.
18. Rice, J.B. & Caniato F. (2003). See endnote 3.
19. Poirier, C. C., & Quinn., F. J. (2004). How are we doing? A survey of supply chain progress. *Supply Chain Management Review, 8*(8), 24.
20. Deloitte Research. (2004). *Prospering in the Secure Economy.* New York: Deloitte Research.
21. Enderwick, P. (2001). Terrorism and the International Business Environment. *AIB Insights Special Electronic Issue 2001*, 1-6.
22. Rice, J.B. & Caniato F. (2003). See endnote 3.
23. Courtney, H., Kirkland, J. & Viguerie, P. (1997). Strategy under uncertainty. *Harvard Business Review.* 75(6), 67-79.
24. Courtney, H., Kirkland, J. & Viguerie, P. (1997).See endnote 23.
25. Miller, K.D. (1992). A Framework for Integrated Risk Management in International Business. *Journal of International Business Studies.* 23(2), 311-332.
26. Miller, K.D. (1992). See endnote 25.
27. Shrader, R.W. & McConnell M. (2002). Security and Strategy in the Age of Discontinuity: A Management Framework for the Post-9/11 World. *strategy+business*(26).
28. Deloitte Research. (2004). See endnote 20.
29. Sheffi, Y (2001). Supply Chain Management under the Threat of International Terrorism. *The International Journal of Logistics Management.* 12 (2), 1-11.
30. Lee, H.L. & Wolfe, M. (2003). Supply Chain Security Without Tears. *Supply Chain Management Review.* 7(1), 12-20.
31. Lee, H.L. & Wolfe, M. (2003). See endnote 30.
32. Sheffi, Y (2001). See endnote 29.
33. Enderwick, P. (2001). See endnote 21.
34. Prahalad, C.K. & Bettis, R.A. (1986). The Dominant Logic: A New Linkage between Diversity and Performance. *Strategic Management Journal. 7(6),* 485-501.
35. Harper, N.W.C. & Viguerie, S.P. (2002). Are You Too Focused? *The McKinsey Quarterly, 2002 Special Edition: Risk and Resilience.* 29-37.
36. Shrader, R.W. & McConnell M. (2002). See endnote 27.
37. Heijden, K. van der. (1996). *Scenarios: The Art of Strategic Conversation.* New York: John Wiley and Sons.
38. Schwartz, P. (1991). *Scenarios: The Art of the Long View.* New York: Doubleday.
39. Deloitte Research. (2004). See endnote 20.
40. KPMG (2001). *Managing Business Continuity: Twenty-First Century Challenges for Competitiveness.* Belgium: KPMG Assurance and Advisory Services.
41. Deloitte Research. (2004). See endnote 19.
42. Brunsdon, D. B., & Dalziell E.P. (2005, July). *Improving Organisational Resilience.* Paper presented at the 15th World Conference on Disaster Management (WCDM), Toronto.
43. Mitroff, I., Pauchant, T., & Shrivastava P. (1989). Crisis, Disaster, Catastrophe: Are You Ready? *Security Management,* February, 101-108.
44. Runyan, R.C. (2006). Small Business in the Face of Crisis: Identifying Barriers to Recovery From a Natural Disaster. *Journal of Contingencies and Crisis Management.* 14(1), 12-26.; Spillan, J.E. & Crandall W. (2001). Crisis Planning Among Guatemalan Small Business: The Assessment of Worst-Case Scenarios. *Journal of Business in Developing Nations.* 5(2).
45. Mitroff, I. (2005). *Why Some Companies Emerge Stronger and Better From a Crisis: Seven Essential Lessons For Avoiding Disaster.* New York: AMACOM.
46. SIA (2003). *Research Update.* 1(12) Alexandria, VA: Security Industry Association.
47. Brunsdon, D. B., & Dalziell E.P. (2005). See endnote 42.
48. Rice, J.B. & Caniato F. (2003). See endnote 3.
49. Hodgson, P. & White, R. (2001). *Relax Its Only Uncertainty. Lead the Way When the Way is Changing.* London: Financial Times/Prentice Hall.