Extreme risk management

Introduction

Boards aspire for the product of their deliberations and efforts to lead to enhanced corporate performance outcomes and the effective management of risks that may be encountered by the corporation in progressing its objectives.

Commonly corporations and boards, including through the risk management committee of the board, seek to:

- identify the risks that may impact upon the corporation, the achievement of its strategic objectives and its operations
- identify the causes of those risks
- assess the impact of those risks in terms of likelihood of occurrence and severity of impact
- hierarchically prioritise the importance of the risks to the corporation
- develop strategies to treat, minimise, manage and/or transfer those risks.

Tools and methodologies such as “Risk Management – Principles and Guidelines – AS/NZS ISO 31000 2009” are used by corporations to help them with this task.

With respect to disastrous events and major crises that pose fundamental threats to the existence or business continuity of the enterprise, commonly the risk of these events and their causes are ranked as having very low or unlikely probability of occurrence (“black swan events”), but very high impact or severity if they do occur. When these two factors are blended using risk management tools and methodologies, the typical weighted risk assessment is only “moderate”. Yet the occurrence of such events may impact corporate survival.

In addition, often the cause of the identified risk is wholly, or at least largely, beyond reasonable control and power of the corporation (natural disasters, government risk, very remote supply chain risks, Acts of God, etc).

Often extreme risks do not warrant, or economically justify, specific treatments to address each and every calamitous outcome that might ever impact the corporation.
Points to consider

• An extreme risk response plan is merely part of the corporation’s overall risk management strategy and risk treatment and response means, and needs to be an integrated part of that.

• A sound extreme risk response plan will help the corporation, and those responsible for its direction and management, to act decisively in times of crisis.

• Plans should be simple and pragmatic, with clear chains of command and communication and decision-making protocols.

• Such plans should be “owned” by management but their existence and integrity “overseen” by the Board.

• Such plans should be reviewed and tested periodically to ensure their fitness for purpose should an extreme risk impact the corporation.

Further observations

Extreme risks create complex challenges for corporations and their directors and management, for instance:

• The cause of the risk may be totally remote from the corporation’s own operations but may impact upon the corporation’s supply chain logistics (eg. 2011 Japanese tsunami impacting Japanese motor vehicle deliveries to Australian car dealers).

• The impact of the risk may be destructive to premises, plant and equipment (operating or IT/financial), and/or data (eg. 2011 Christchurch NZ earthquake).

• The cause of the risk may preclude personnel from accessing the business premises to attend to their work (eg. 2011 Queensland floods and Fukushima nuclear disaster).

• The impact of the risk may be detrimental to human health or life (eg. disease pandemics, hazardous material spills).

• The impact of the risk may be severely detrimental to corporate reputation (eg. BP’s Mexican Gulf oil well explosion).

• Rectification and repair of the damage suffered by the corporation to restore business operations may take time;

• Business continuity is often materially compromised for an extended period.

More recent business models have revealed new risks, including extreme risks that can affect the corporation’s business, such as:

• globalisation (24/7/365 everywhere in the world)

• “just in time” inventory and logistics management

• outsourcing of critical components

• supply chain assurance

• IT

• actions that allow financiers early withdrawal of facilities in times of business stress.

In addition, today news of extreme risks, their impact and corporate responses, can travel fast and have major ramifications. For example, social media is perhaps the single greatest new arena that can affect a business and cause immediate extreme risks, primarily to reputation and then indirectly to other areas of a business.
Insurance

Extreme risks are often accepted by a corporation but specific risks are managed though insurance to transfer a potential financial impact of the risk to the insurance company, which in turn effectively shares the risk with its pool of policy holders by virtue of the actuarial determination of the risk and the insurance policy premiums all policy holders have paid.

However, an effective risk transfer and treatment through an insurance solution assumes that:

• the cause of the extreme risk is in fact an insurable event
• insurance cover is available at an economically acceptable price
• the estimated financial impact insured against is an adequate estimate of the loss to the corporation
• the insurance claim and compensation will be processed and paid in a timely manner so that the impact of the extreme event can be rectified swiftly
• money can compensate for less.

Sometimes an extreme risk does not have a very low or unlikely probability of occurrence, in which case it may in the corporation’s best interest to do more to treat or manage the risk, or minimise the severity of its impact.

In these cases, treatment by insurance cover (ie. risk transfer) might not be available, or only be available at a prohibitive insurance premium cost, and even then subject to a myriad of exclusions and conditions. An industrial operation in a flood prone valley would be an example of this.

Common methodologies to address extreme risks

Although extreme risks are many and diverse, with each having its own discrete cause and effect, there are methodologies which corporations can adopt across a broad range of risks and their causes to minimise the impact to the corporation, whether it be a “black swan” or an extreme risk event with a higher likelihood of occurrence.

The aim is to identify threats, minimise and treat their impact, limit the scope of their damage, recover from the impact of the event as soon as possible, minimise business discontinuity and maintain corporate reputation, standing and integrity. This will help maintain competitive advantage and ultimately ensure the business remains viable as a “going concern”.

The template in Schedule A contains key issues to consider when developing an extreme risks response plan, as well as detail to assist corporations to customise the contents of the template for their own unique needs and circumstances.
Schedule A

Steps in developing an extreme risk response plan

<table>
<thead>
<tr>
<th>No.</th>
<th>Step</th>
<th>Commentary</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Understand the extreme risk landscape</td>
<td>(a) Identify the nature, cause and impact of extreme risk events that may affect the corporation or its operations.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(b) Consider any common themes in the nature, areas and scope of impact.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(c) Identify the core or critical areas of sensitivity of your corporation’s affairs and operations, with focus on those that may be impacted by the extreme risks from your analysis in (a) and (b).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(d) From this analysis prioritise the most sensitive areas and functions.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(e) Consider what prospective protective, strategic alternate and remedial actions and steps may need to be taken to mitigate the impact of those risks and to preserve and/or restore the functions and operations of the corporation impacted thereby.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(f) “Risk Management – Principles and Guidelines – AS/NZS ISO 31000 2009” is a useful tool to assist in this exercise.</td>
</tr>
<tr>
<td>2</td>
<td>Consider the extreme risk impact and its management</td>
<td>(a) Assume that each different extreme risk event has respectively occurred.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(b) Develop scenarios reflecting what the corporation’s environment (physical and virtual) could look like with each event.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(c) With a detached and objective perspective, consider how the corporation would like to emerge from each event in terms of people, assets, data, resources, operations and reputation.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(d) In particular, focus on how each event can be managed and business continuity preserved, without prejudicing the broader legal and ethical responsibilities the corporation and those responsible for its direction and management have for its stakeholders.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(e) Particular consideration needs to be given to liability risks for the corporation and its directors and officers including:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• duty of care responsibilities especially to its personnel and broader stakeholders</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• contractual obligations and responsibilities</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• insurance notification requirements</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• environmental responsibilities</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• reputational exposure and its management.</td>
</tr>
<tr>
<td>No.</td>
<td>Step</td>
<td>Commentary</td>
</tr>
<tr>
<td>-----</td>
<td>------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| 3   | Document the extreme risk response plan from the following five perspectives: | (a) Command and control  
(i) Crisis periods require military style discipline, leadership, communication, decision-making and devolution of authority.  
(iii) Consider the following:  
  • who will take primary charge, and who will be the backup in case of redundancy  
  • where will the control be centred from, and what is the alternative in case the primary centre is also adversely impacted  
  • what special authority is conferred to whom, so that decisions can be taken and acted on promptly (the convening of formal board meetings in such circumstances may not be practical).  
(iv) Ensure the control centre location is fit for purpose and outfitted with appropriate information and communications technology (I&CT).  
(b) Communications  
(i) Communications over this period will be vital, not only in terms of I&CT infrastructure but also reporting and information flow:  
  • to and from the corporation's personnel and consultants  
  • with respect to any “real time” or critical need functional operations of the corporation  
  • to and from the corporation and any relevant regulator  
  • to and from the corporation and the media  
  • to and from the corporation and its broader stakeholders.  
(ii) There are obvious overlaps between “communications” and “command and control”.  
(iii) Continuously updated lists and details of contact particulars (including emergency contacts) of all personnel and key consultants, especially those holding vital offices within the corporation, are important.  
(iv) Prepare a professional community and media relations strategy ready to be used.  
(c) Marshalling resources  
(i) In the event of an extreme risk impact, many of the corporation's traditional resources may be compromised. In order to best respond to the event it will be necessary to marshall and co-ordinate the utilisation of resources from other areas of the corporation's operations and/or from outsourced providers.  
(ii) A plan for standby arrangements for corporate resources should be prepared. |
<table>
<thead>
<tr>
<th>No.</th>
<th>Step</th>
<th>Commentary</th>
</tr>
</thead>
</table>
| 3   |      | **Document the extreme risk response plan from the following five perspectives:**  
|     | 1.   | command and control of management of the extreme risk event  
|     | 2.   | communications  
|     | 3.   | marshalling resources  
|     | 4.   | damage control  
|     | 5.   | business continuity and recovery. |
|     |      | **(d) Damage control**  
|     | (i)  | Responses which address all of the following are needed:  
|     |      | • risk impact containment  
|     |      | • damage control  
|     |      | • consequential liability and risk contagion more broadly to the corporation and to third parties.  
|     | (ii) | Damage control includes (without being exhaustive) risks to:  
|     |      | • people  
|     |      | • property  
|     |      | • plant and equipment  
|     |      | • I & CT and other systems  
|     |      | • supply chain  
|     |      | • finances  
|     |      | • reputation and standing.  
|     | (iii)| Plans need to be sufficiently flexible so that both immediate/short term damage control is balanced with the longer term recovery prospects for the corporation.  
|     |      | **(e) Business continuity and recovery**  
|     | (i)  | Beyond the health and safety of the corporation’s personnel, a primary driver of the plan must be to help assure the maintenance of business continuity.  
|     | (ii) | Business continuity implies:  
|     |      | • an interim sustainability of corporate organisation, operation and management control during the period that the event has compromised the corporation;  
|     |      | • the progression from the compromised position back to full recovery.  
|     | (iii)| The plan should therefore dwell not only in dealing with the crisis, but also in dealing with managing the recovery and transition back to full production and operational capacity once the immediate impact of the event has been managed.
<table>
<thead>
<tr>
<th>No</th>
<th>Step</th>
<th>Commentary</th>
</tr>
</thead>
</table>
| 4  | Sharing and maintaining currency of the plan | (a) Guidance manuals  
  (i) In addition to the overall plan, complementary guidance manuals should also be prepared to support the implementation of the plan.  
  (ii) These manuals should be more task or function-specific to enable operative personnel to undertake critical tasks with assurance.  
(b) Plan/manual availability and control  
  (i) Subject to corporate security needs, copies of the plan and complementary manuals need to be available to the right people.  
  (ii) Version control measures helps to ensure that all copies of the plan/manuals in circulation are contemporary.  
(c) Review – making the plan a “living” document  
  (i) The plan and any accompanying manuals must be reviewed regularly. In the dynamic life of corporate endeavour circumstances constantly change.  
  (ii) In particular, the positions, personnel and contact details of people internally and externally to the corporation, and emergency, utility and regulatory authorities constantly change and need updating.  
  (iii) Likewise the systems, management process and organisational management structure of the corporation are likely to continuously evolve. |
| 5  | Training and Rehearsals/Testing | (a) Training  
  (i) A well considered and documented extreme risk plan is supported by an extensive training regime.  
  (ii) Periodic refresher training assists preparedness.  
  (iii) Follow up training is required after each major update and review of the plan.  
(b) Rehearsals/Testing  
  (i) Practical periodic rehearsals of the plan train personnel and also “test” the plan in practice, often revealing “bugs” that need to be eliminated for the soundness of the plan. |
<table>
<thead>
<tr>
<th>No</th>
<th>Step</th>
<th>Commentary</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>Cultural Awareness</td>
<td>(a) In addition to the analysis, development, documentation, communication, training, rehearsal and testing of the plan, awareness of the plan and what it achieves is vital.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(b) The challenge in developing this awareness is that by its very nature, the corporation hopes never to need to action it, and many corporations never will need to do so.</td>
</tr>
</tbody>
</table>

Further information concerning disaster planning, business continuity planning and crisis management can be found in the following Company Director magazine articles:

- **Longford crisis Management – an opportunity lost**
  Bernd Rieve, August 1999
- **Crisis myths and how to debunk them**
  Steve York and Scott Farquharson, March 2000
- **The Rules of Engagement**
  Bruce C Wolpe, Dec 2005/Jan 2006
- **How to manage a Crisis**
  Giles Parkinson, July 2006
- **Crisis Denial**
  Euan Campbell, September 2010
- **Preparing for Disaster**
  Zilla Efrat, November 2010
- **Disaster Proofing your Business**
  Daryl Wright, March 2011
- **Preparing for Disaster**
  John Colvin, April 2011
- **Disaster Alert**
  Domini Stuart, April 2011
- **Tales from the Disaster Zone (Japanese tsunami)**
  Zilla Efrat, June 2011