Strategic Risk Management – is it doable, sensible or desirable?

Business leaders and government bureaucrats around the world are being told that they need to do much more in understanding and implementing strategic risk management. They are told that the modern business environment is so complex that survival is increasingly tied to good risk management practise. They are told the answer lies in embracing complex and integrated risk management processes such as Enterprise Risk Management, and integrating them into all other processes within the organisation. Even the new international risk standard, ISO 31000 Risk Management Principles and Guidelines, page v, recommends that organizations develop, implement and continuously improve a framework the purpose of which is to integrate the process for managing risk into the organization's overall governance, strategy and planning, management, reporting processes, policies, values and culture.

I advise organisations differently. By all means, let's applaud the ISO for wanting to raise the understanding and engagement of risk management but let's not overcomplicate the response required by organisations to effectively understand and implement strategic risk management. The more I see of large organisations failing to identify and prepare for strategic risks, the more I recognise the solution isn't complicated and integrated risk management processes. Rather, I think the solution involves the ability to look beyond the current environment in which your organisation exists and to conceptualise the potential advances, opportunities, threats and 'business killers' that will surely come your way. How quickly you conceptualise these risk scenarios and then ground their impact in your current environment, will mark future winners from losers.

Four examples demonstrate my point. The Canberra bushfires of 2003, the terrorist attack on the JW Marriott Hotel in Jakarta in 2009, the Iceland volcanic eruptions in 2010, and the Transocean rig fire in the Gulf of Mexico in 2010. Evidence to the Coroner's investigation by the Emergency Services organisation in Canberra confirmed that risk management was well understood and effectively implemented. Given this level of risk management preparedness, how did the fire authorities decide not to fight the fire caused by the lightning strike in the Brindabella Ranges? Was it the fact that no one conceptualised the possibility of that distant lightning strike combining with unusual weather conditions to become a conflagration that burnt into Canberra, killed four people, seriously injured hundreds, destroyed or seriously damaged 400 homes and cost millions of dollars? The JW Marriott hotel was first attacked by terrorists using a vehicle bomb in 2003. It was attacked for a second time in 2009 by a terrorist using a body bomb that was assembled in the hotel with insider support. How was a successful second attack mounted given that JW Marriott employed risk management processes and new security measures and processes were implemented after the 2003 attack? Did the hotel's security preparedness after the first attack become vulnerable over the years, or did the hotel fail to conceptualise the type of scenario that eventuated in 2009? The Iceland volcanic eruptions in 2010 closed European airspace for almost a week and cost airlines operating in Europe hundreds of millions of dollars. In the example of British Airways (BA), was the possibility of UK airspace closed for a week conceptualised? If it was, why for example didn't

BA have strategic plans to locate part of its fleet in southern Europe and agreements with train and ferry operators to shift passengers between that location and London? Finally, when the Transocean oil rig exploded and sunk in the Gulf of Mexico in 2010 why didn't BP (the well owner) have tested plans and procedures to quickly cap the exposed well? These four examples are instances of significant strategic risk management failure. Not because the target organisations didn't have risk management in place, but because they didn't conceptualise the risk event and then work out an appropriate response.

If the answer is to conceptualise the risk scenario, how should organisations do that? I think the answer is to implement three processes: firstly, foster a wide-ranging and uninhibited scenario generation regime; secondly, import the scenarios into a simple risk assessment tool that supports the processing of the scenarios to identify changes in likelihood and risk; and thirdly, spend the money and effort to confirm you have a proven risk mitigation response to the risk.

Developing a wide-ranging and uninhibited scenario generation regime requires an organisation to engage its personnel in the study of its environment. That will involve some training on how to undertake scenario generation, encouragement to think 'outside the box', and remuneration for relevant scenario generation. Scenarios should identify signals, indicators, or events that indicate an organisation is entering or about to enter a period of change that signals either opportunity or threat. The regime must have the flexibility to quickly add new scenarios for collective consideration with existing scenarios before the event is experienced or in the least desirable outcome, as an event unfolds. The regime should provide for simple and easily digested reports that can be communicated, preferably immediately via a medium like the Internet, to anyone responsible to input the scenario into the risk tool or to implement the risk mitigation response.

Importing the likely scenarios into a simple risk assessment tool brings the scenarios and their attached likelihoods together with the consequences to identify risks or opportunities. Most risk standards say very little on likelihood other than it's a measure of probability. If you agree with my premise that scenarios are fundamental to effective risk management, then you need a much deeper understanding of the likelihood of each scenario. By breaking likelihood into sub-elements such as intent, capability and vulnerability, you gain a better understanding of the potential for the scenario to confront your organisation. My contention is that a simple risk assessment tool doesn't require linkage into all aspects of an organisation's overall governance, strategy and planning, management, reporting processes, policies, values and culture. These important parts of an organisation's daily routine (in this context) only distract attention from the real risk game; identifying the scenario and its likelihood, and analysing its potential for opportunity or threat.

Spending the money and effort to confirm you have a proven risk mitigation response to the risk before it impacts would appear to many to be wasteful in time, resources and focus. But consider the Board of BA as the CEO might have advised them that they had no effective response to the closure of airspace except to attempt compensation from the UK Government. Or BP as they scramble to develop any response to the unregulated flow of oil in the Gulf of

Mexico that is negatively impacting their reputation and potentially costing billions of dollars to remedy. Press reports indicate that the dome built to try to cap the oil well had not been tested by BP at the required depth before. In hindsight, such testing now looks necessary no matter the costs.

The biggest challenge posed to any organisation is strategic risk. You will not understand the components of strategic risk if you don’t understand the range of scenarios that will eventually confront your business. By embracing complicated business practices, you lose the perspective on what really counts in strategic risk management: informed early warning; easily understood risk processes; and well understood and effective risk mitigation.