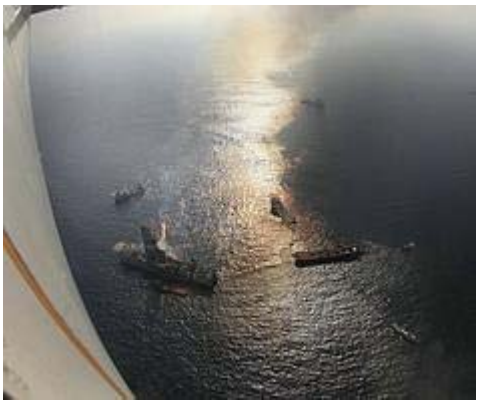
Managing catastrophe

PUBLISHED: 04 Aug 2010 01:47:23 PRINT EDITION: 5 Aug 2010

Leo D'Angelo Fisher

One company's catastrophe can be another's gain. When Brisbane family owned frozen pie and sausage roll manufacturer Tastee Products was destroyed by fire last year, its empty spot in supermarket freezer cabinets was promptly filled by its much bigger rival Patties Foods, manufacturer of Four'N Twenty pies.



In deep water: BP's response to and management of the Deepwater Horizon oil spill off the Louisiana coast has been widely condemned.

At the time, Patties was desperately rebuilding its market share. Some poor management decisions after its 2006 public listing had caused its dominant market share to plummet. Patties has since regained its No. 1 spot, in part, chief executive Greg Bourke told shareholders, because of the Tastee fire, "an unexpected event out of our control".

Catastrophe doesn't discriminate. It can strike at any time and can destabilise businesses large and small.

Nor are threats just physical outside events. Think of Barings, Britain's oldest investment bank, which evaporated in a weekend in February 1995 because of the unseen doings of a rogue futures trader in its Singapore office – and was sold for a pound to Dutch bank ING.

BP, which last year was the world's fourth largest company, knows all about fires as well. Its chaotic response to the catastrophic explosion and oil spill in the Gulf of Mexico is hardly the sophisticated reaction one might expect of a vast oil company.

BP's technical feats in since plugging the deep-water well have been unparalleled. But this has hardly made up for the lack of planning, slow initial reaction, buck-passing to contractors, reports of cost-driven operational management and worst of all, a series of public relations howlers from the top of the company.

Who can say what BP's former chief executive, Tony Hayward, was thinking when, a month after the explosion, he predicted that the environmental impact would be "very, very modest". Or when he told an incredulous congressional committee in Washington that "I wasn't involved in any of that decision making" that resulted in the choice of a cheaper but riskier well design.

With a battered reputation and liabilities that will run into many tens of billions of dollars, the consequences for BP of this catastrophe won't be pretty. Its market capitalisation fell 40 per cent at one point, to half that of rival Exxon Mobil. Unwelcome possibilities include sales of assets to its competitors or even the threat of takeover. In the meantime, many consumers, investors and company executives are voting with their feet.

So how was this oil leviathan brought to the brink of ruin by a disaster that should not have been beyond its anticipation? Why do company-threatening events happen so often?

Scenario planner David Andrew is not surprised. A consultant with Perth strategist Virtual Consulting International , he works with senior executives from the energy and resources sectors to help map future scenarios, including events with the potential to damage or destroy a company.

The process involves sitting down with chief executives and their senior leadership teams to workshop potential doomsday scenarios – from internal system failures to environmental disasters to economic and political upheavals. Andrew says executives in these sessions are usually reluctant to consider the unthinkable.

"We have to tease them out of their comfort zones to uncover things they otherwise wouldn't have thought about," he says. "The purpose of getting them into the room is to help them expand their minds out of today and out of their own organisations. When you're inwardly focused you're unable to respond to unexpected events."

Scenario planning is as much about preparedness as it is predicting events.

"Scenarios identify the signposts, the leading indicators that a company is heading for a devastating event that could impact the business," Andrew says.

"Scenarios are layered so that participants understand how one event can lead to something else. Understanding impacts at one level prepares you for other impacts and how you'd react to them."

Disasters of the magnitude of the Gulf of Mexico oil spill and the global financial crisis have raised questions about the effectiveness of risk management. It's an aspersion rejected by the Risk Management Institution of Australasia .

Ted Dahms , a Brisbane risk management consultant and principal author of an RMIA white paper, *Organisational Resilience* , says the financial crisis revealed "the failure to understand and apply sound risk management principles". Banks and financial institutions that should have treated risk management as part of their corporate governance were treating it instead as a separate function unconnected to the rest of the organisation.

"No part of an organisation works in isolation," he says.

Even the most ardent proponents of risk management admit that picking risk can be an uncertain science. "Elements of uncertainty that can be anticipated are in themselves subject to uncertainty due to the complexity of relationships within and without an organisation," Dahms explains.

In its annual risk management survey released in March, risk and insurance group Aon Australia ranked the top 20 risk concerns. At No. 18 was "natural disasters and climate change". The next month, the Eyjafjallajokull volcano in Iceland erupted, creating the worst disruption to global air travel since the terrorist strikes on US soil on September 11, 2001.

Qantas lost $10 million during the five days of disruption immediately following the eruption and chief executive Alan Joyce admitted to *BRW* at the time that "the volcano would not have been on the risk register".

Jason Brown , chief risk officer at QBE Insurance Group , believes it pays to be prepared for any credible scenario.

"The real challenge is for organisations to consider the improbable as possible and to establish processes that will respond appropriately, and to rigorously test them,"
he says.

QBE practices what it preaches. The insurer, which provides cover for oil rigs, recently announced to relieved shareholders that it
had reinsurance protection to minimise its exposure to large claims arising from the
Gulf of Mexico disaster.

For the third year in succession, "brand and image" topped Aon's list of risk concerns. At such a volatile time this would seem a fatuous concern but as Aon chief executive Steve Nevett points out, the concern about brand and image presupposes the effect of other events on a company's reputation. "It's an effect risk rather than a primary risk, whereby brand and reputation suffer as a result of another risk coming to the fore," he says.

Toyota's accelerator pedal recall – and the company's initial reluctance to admit there was a problem – exemplifies how even a peerless brand reputation can suddenly come under threat when a company loses control of events.

Matthew Curtis , group manager of security at consulting firm GHD , specialises in security and emergency management.

Before becoming a consultant, he worked in diplomatic and national security roles with the Australian government. It's the kind of background that enables Curtis to discuss organisational resilience in the face of catastrophe in a matter-of-fact manner.

"Resilient organisations tend to be those that are able to meet their key operational requirements when faced with disaster or challenging circumstances," he says. They are also well informed.

"A manager responsible for security or protecting corporate good has a very powerful tool at his disposal: intelligence. It's important for that manager to cultivate relationships with people in the know in other organisations, in government and with stakeholders," Curtis says.

"To make sure intelligence is optimised, it's important to have a methodically sound process that enables you to be informed of risk, to identify, assess and prioritise risk and to shed light on vulnerabilities."

The shape of that process can be the sticking point. Just as some experts lament that some organisations marginalise risk management by making it a discreet operational function, the managing director of Canberra risk management consultant Intelligent Outcomes Group , Mike Dunn , says many companies have made their response to risk management too complicated.

He is critical of complex integrated risk management systems – recommended in the ISO 31000:2009 international risk management standard and generally considered best practice – which seek to infuse responsibility for the management of risk into every facet of an organisation.

“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,” he says.

The fact that international airlines did not have contingency plans for the Icelandic volcanic eruption and the difficulties faced by BP in the Gulf of Mexico are examples of risk management failure, “not because these companies didn’t have risk management systems in place,” he says, “but because they weren’t able to conceptualise risk events and work out an appropriate response”.

Dunn, a former director of military intelligence in the Australian army, is an advocate of scenario planning to identify threats and their likely consequences.

Scenario planning and developing risk-mitigation strategies is expensive and requires “buy in” from a company’s leadership, he says, which is why even companies with a formal commitment to risk management can be caught flat-footed when disaster strikes.

“There’s got to be a belief, from the CEO and chairman down, that these scenarios make sense, even if they’re only going to happen once in 100 years,” he says.

“The view tends to be, ‘this is unlikely to happen so it doesn’t make sense to spend so much money on mitigation’. What they should be saying is, ‘if we don’t follow through, the consequences for our business, if this scenario does occur, would be catastrophic’.”

A 2009 report by the Economist Intelligence Unit, *Beyond box-ticking: a new era for risk governance* , says the global financial crisis has highlighted the importance of moving beyond a cosmetic approach to risk. “A box-ticking approach to the management of strategic risk is, in a post-crisis environment, more likely than ever to lead to corporate ruin,” the report warns.

The global survey found growing awareness about the importance of risk management, but not always the commitment to match. Even when companies recognise their deficiencies in risk management, they are unlikely to invest in necessary improvements (for example, in data, technology and recruitment), the survey found. Among other findings, many risk managers who seek a broader strategic role find themselves overwhelmed by compliance work and attempts to build an effective risk culture is often undermined by a lack of leadership support.

Reflecting this ambivalence about the role of risk management, just 35 per cent of companies in the survey had a chief risk officer. Among those that did not, more than half had no plans to recruit one. (The Aon survey found that 31 per cent of Australian organisations have a chief risk officer, which is expected to decline “as risk management becomes further embedded within organisations”.)

The EIU report suggests it is up to chief risk officers to make their presence felt. “If ever there was a time for chief risk officers to force their way into the boardroom and demand that the risk function be represented at the top table, surely it is now,” it says.

QBE’s Brown believes the role of chief risk officers is likely to become “more crucial” in highly regulated sectors such as banking and insurance but elsewhere the role has a less certain future.

“For those industries with less prudential-based regulation, I see the prevalence of CRO appointments aligning to some degree with the rise and fall of economic and investment cycles and the number of large-scale risk events that occur and are later forgotten,” he says.

Robert Stribling , group chief risk officer at banking and insurance group Suncorp , sees his role as being a “risk champion”, driving an awareness of risk throughout the organisation. He considers culture a vital component of successful risk management.

“One can mandate that risk management systems are put in place but if the culture is not right, having those systems won’t guarantee effective risk management,” he says.

“Within many organisations a culture exists where people only like to pass good news up to management; they keep the bad news to themselves and hide mistakes. Sometimes, it’s these seemingly inconsequential mistakes that can blow up an organisation.”

Stribling says the global financial crisis should not be viewed as an indictment of risk management but he agrees that it did expose weaknesses in how some of the world’s biggest companies managed risk.

“The failure of risk management, in many cases, was all about execution,” he says. “In many companies, risk management had become process-bound and was quite superficial.”

Another deficiency exposed by the financial crisis was the extent to which risk management tended to focus inwardly within each company. “Risk managers were not really thinking about the activities of the company within a broader, system-wide context,” he says.

“The GFC has reminded us all that risk management needs to focus not just internally within the organisation but also on what’s happening externally, outside and around the company.” “In hindsight, it’s common sense, but it’s a principle that for many financial services companies just got lost over time.”

Seeing the whole picture

A Canberra think tank, the Australian Risk Policy Institute , says the GFC, Gulf of Mexico oil spill and disruption to air services following the volcanic explosion in Iceland, have exposed the weakness of risk management systems. ARPI has proposed a new model for managing risk, which it believes should be mandatory.

ARPI president Tony Charge says recent catastrophic events demonstrate existing risk management systems often fail to ensure decision-makers have information they need at critical times.

“A critical breakdown in risk management is that chief executives and boardrooms are not getting the full picture,” he says.

“Instead, risk is being viewed at the business unit level rather than in terms of implications for the whole organisation.”

The ARPI risk policy model comprises three components: risk policy to “authorise, inform and define” risk management as a strategic business process; risk management to identify and assess risks; and risk governance to ensure “articulation, adoption and implementation” of risk policy.

The model requires organisations to broaden their sources of information and risk identification by including stakeholder networks in risk management processes and factoring in systemic risks in society, government and business. It includes vulnerability as a risk criterion.

Charge says adoption of the model would provide rules of engagement for sharing information and would help restore confidence in risk management.

“The model has been designed to provide decision-makers with information that otherwise might not be recognised,” he says. “Information and knowledge can’t always prevent things from happening but with information and knowledge situations can be better managed.

“If you consider the GFC, information was available but was not brought to the attention of decision-makers, allowing events to spin out of control. The model would fill that void.”

Charge would like to see the model mandated as a principle “but not at the process level”.

He believes the model is applicable to all businesses, government, community and not-for-profit organisations.

The Australian Securities Exchange’s voluntary corporate governance code recommends that companies should establish a “sound system of risk oversight, management and internal control”.

A risk too far

Perth iron ore explorer Sundance Resources is tragic proof of what risk management consultants regularly tell sceptical clients: just because a potential risk seems improbable doesn’t mean it won’t happen. On June 19, an aircraft chartered by Sundance went missing in west Africa, en route to its iron ore project in Congo. Aboard the plane was the company’s chairman, Geoff Wedlock, chief executive Don Lewis, company secretary John Carr-Gregg, and non-executive directors Craig Oliver, John Jonesand Queensland mining magnate Ken Talbot.

The mangled aircraft was found in dense jungle in the Congo two days later, with all 11 on board confirmed dead. Rising above the tragedy was the obvious question: why did the company’s entire leadership team travel on the same plane?

George Jones (no relation to John), who came back from retirement as Sundance chairman to head a three-man de facto board, says the board did not have a formal risk policy on air travel. The company was mindful of risk management, “but our risk management planning didn’t contemplate losing the whole board”, Jones told *BRW* a few days into the unfolding tragedy.

If Sundance’s risk assessment was misplaced, its crisis management after the event was case-study perfect. Within three hours of being informed of the plane’s disappearance, Jones, who retired as chairman in August 2009, lawyer Michael Blakiston and investment banker Adam Rankine-Wilson formed an emergency advisory committee

and chief financial officer Peter Canterbury was appointed acting chief executive.

A public relations company issued regular bulletins about the progress of the search, recovery and repatriation of the dead, Jones made himself available for round-the-clock media interviews and the ASX agreed to the company's request for a suspension of trading from June 21 .

The suspension was lifted on July 19; on the first day of trading shares fell 1¢ to 12¢.

The company has appointed a new board – headed by Jones – and a search is under way for a new CEO. Jones says there will be a formal review of Sundance's risk management policies.

Containing the aftermath

Matt Horan has three rules for saving a company's reputation from crises: avoid them in the first place; plan a response in case one happens anyway; and in that unhappy event, bin the plan and wing it.

A senior communications adviser at Cato Counsel and former news editor at *The Sunday Telegraph* , Horan is surprised by the failure of many companies to anticipate the harm that, say, a workplace death, can do to their standing with employees, customers, investors and politicians.

"You might have procedures for informing the families affected," he says.

"But what will you do after that? Offer counselling? That's great. But what will you do if five cameras turn up outside the families' doors?"

Horan says asking such questions ahead of time is more important than the answers written into a crisis management plan.

"Plan for everything. When it happens, throw the plan out because it will rarely fit," he says.

"If you have done the planning on a hypothetical incident, at least you have the structures down in how you deal with it."

This is critical in the era of Facebook, Twitter and other social media.

"In the past, you normally had a few hours before you had to respond," he says. "You could sit back and ask, 'How are we going to deal with this?'

"But with the velocity of social media, you actually need to have these plans already done."

Anthony Tregoning, managing director of Financial and Corporate Relations advises companies to build up a bank of goodwill with stakeholders.

"The seeds of reputational damage are sown before a crisis happens," he says. "If a business has a strong goodwill bank on which to draw, it can withstand negative publicity far more effectively."

This especially applies to government relations. BP failed to open lines of communication with the Obama administration earlier, he says.

Operational issues – in BP's case, stopping the oil leaking – can overwhelm top managers. There needs to be a dedicated team "focused totally on reputation".

"The fact that the government has attacked the company as it has, indicates that BP didn't engage with the government either as transparently or at the right level as it should have done," Tregoning says.

BP's travails also raise the issue of how frank companies should be.
Horan says it depends on the nature of the incident.

"On some incidents, you should be very open," he says. "On others, you need to ask whether the information impacts on your commercial strategy."

Here social media can work in a companies' favour, Tregoning argues.

"BP is using social media – especially YouTube – to show what the company is doing to stem the leak," he says. "This way it fills any information vacuum with graphic messages, backed by video, that it is doing all that is possible.

"Social media can give you the opportunity to get across your point of view and to counter misleading information."

BRW

Related News

Topics Accidents & Emergencies, Environment

Create an alert

Click on the links below to create an alert and receive the latest news as it happens

Topics Accidents & Emergencies, Environment