

# INSURANCE & RISK MANAGEMENT

## RISK FACTORS

# Insurance one part of a greater whole

The key to successful risk management is to follow a formal risk management framework and strategy, writes **Anthony Davies**.

Mention risk management and insurance in the same breath and many people will assume they're the same thing. They're not. The two aren't synonymous, there's a significant difference; risk management is far broader than insurance, which is just one part of it.

"Insurance covers some of the financial consequences of some of the risks you're exposed to," says Chris Peace, managing director of Wellington consultancy Risk Management and deputy-chairman of the NZ Society for Risk Management.

Depending on the type of company you're running, he says the proportion of your risks that are insurance could be as low as 10%.

That's reinforced by the results of a global survey conducted last August by insurance broker and risk management consultancy Marsh. The firm asked 110 senior managers how they review and manage risk and what they think the five main risks to their businesses are.

The top five risks highlighted were:

- Loss of data;
- Disruption to the business after a major incident;
- Losing key staff to competitors/inability to retain staff;
- Lack of strategic planning;
- Failure of systems security.

Two years ago, the top five risks were:

- Increased competition;
- Non-compliance with legal and contractual obligations;
- Losing staff;
- Loss of data;
- Disruption to the business after a major incident.

Marsh NZ chief executive Kirk Williams says what has changed is an appreciation by

business of the significance of intellectual property and risks associated with not protecting it properly.

Take computer systems. You can easily insure the physical assets, but the data they contain is far more crucial.

An insurance payout will replace computers but it won't restore or replace lost data. To do that you need efficient back-up systems. And the keys to a good back-up system are duplication and separation, says risk management commentator Patrick Caragata in his book *Business Early Warning Systems*, which identifies and analyses common features in many of the 20th century's greatest disasters.

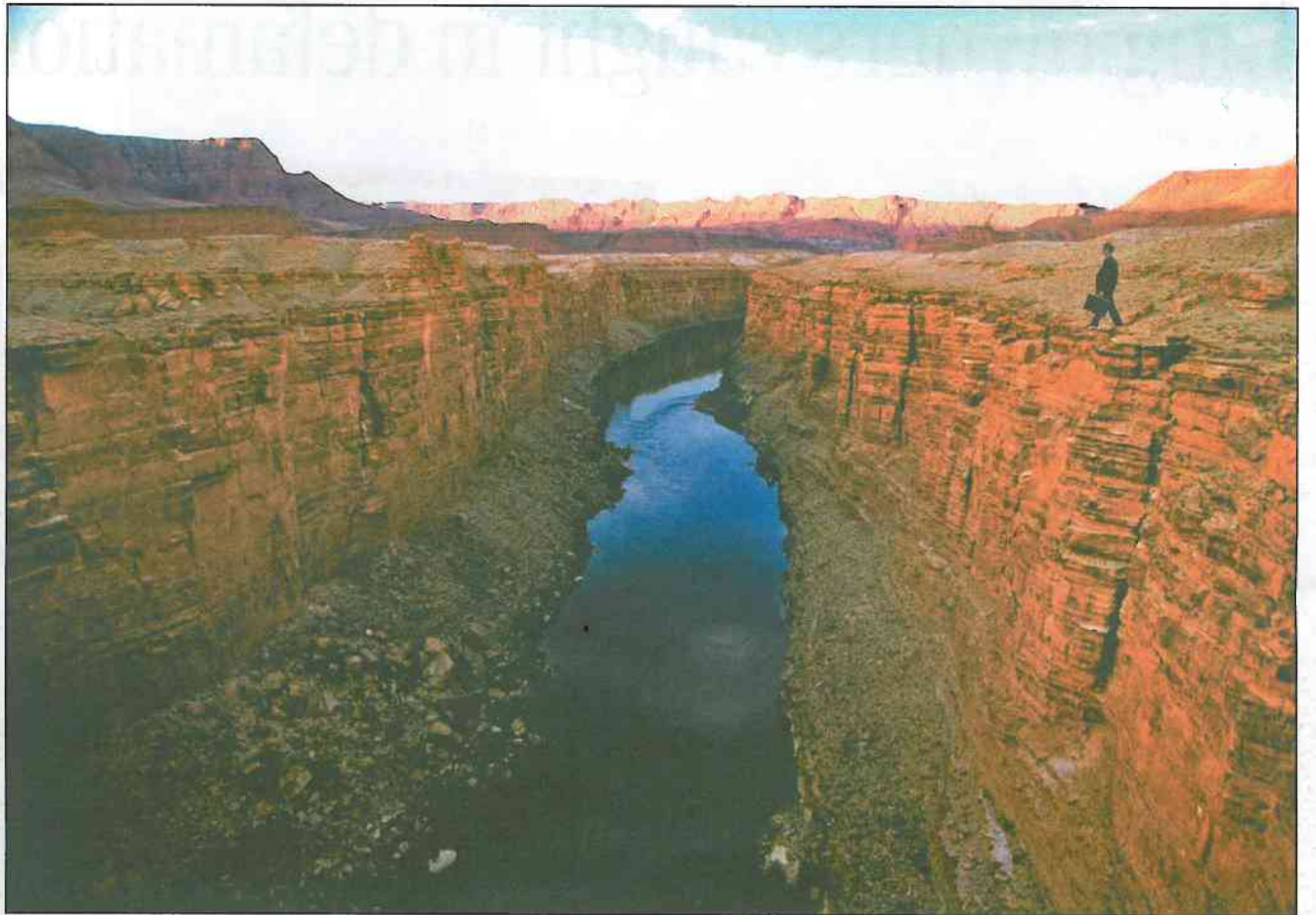
### An insurance payout will replace computers but it won't restore or replace lost data.

Duplication is the easy part, he says, but failing to properly address the separation issues has failed to prevent many crises where the incident which disrupts or destroys a vital system or piece of equipment also takes out the back-up.

The Tokyo Stock Exchange was a classic case of what not to do.

In 1989 it was revealed the exchange's main and back-up computers sat side-by-side in the same room in a location which was flattened in a 1923 earthquake. If another similar earthquake struck, all official records of share ownership would have disappeared. Fortunately, the back-up computer was relocated after the story became public knowledge.

The Tokyo story illustrates how one simple oversight



The great divide: Don't leave your business vulnerable to sudden disasters.

FAIRFAX/GREG NEWINGTON

could have serious consequences.

Or take the Piper Alpha disaster. On July 6, 1988, it was

destroyed by an explosion and the resulting fire killed 167 men. At the time it was the largest North Sea oil production platform and was thought to have state-of-the-art risk management and safety programme in place. It did and it didn't.

While the programme was comprehensive in places, the problem was some risks were overlooked because they weren't on anyone's list. For example, one factor contributing to the scale of the inferno was that a nearby platform, the Tartan, continued pumping gas into the heart of the fire until the heat ruptured the pipeline. While the Tartan's crew could see Piper Alpha was on fire, they didn't have the authority or ability to shut off production and isolate Piper Alpha.

No matter how careful or

thorough you are, there will inevitably be some risks which get overlooked. Allan Morris, a risk management consultant and deputy-chairman of business risk management franchise Triplejump, illustrates the point. Ten years ago he and his colleagues profiled a mid-sized manufacturing and exporting business to catalogue every risk it was exposed to. The list ran to more than 700, and probably only 20% of them were insurable.

"A lot of small businesses have risks they don't know about," he says. "They run their businesses by the seat of their pants and they buy insurance thinking it's a panacea. But it's not, it's only part of a solution."

He adds their failure to adequately address risk management issues are often compounded by not having or being able to afford the procedural disciplines and governance frameworks which larger businesses, especially listed businesses, have in place.

Peace says the key to successful risk management is to follow a formal risk management framework and strategy. Given that no companies or organisations are identical, your starting point should be process and principles rather than someone else's list.

Peace defines risk as "something that will impact on your objectives". Businesses first need to know what their objectives are. "If you have no objectives, you don't know what your risks are," he says.

He suggests a good place to start is the risk management standard jointly developed by Standards Australia and Standards NZ, AS/NZS4360 (see the NZ Society for Risk Management's website, [www.risksociety.org.nz](http://www.risksociety.org.nz)), which will shortly be recognised as an international standard, ISO3100-Risk Management.

The standard defines risk management as "the culture, processes and structures which are directed towards the effective management of potential opportunities and adverse effects".

It outlines a four-stage process: establish your context,

identify risk, analyse and evaluate them and then treat them.

Morris stresses it's important not just to identify risks, but also to assess and quantify their likely impact, and the priority risks to address should be those which are "high consequence and high probability".

Wellington practitioner John Sloan, principal of Sloan Risk Management Services, advocates a commonsense approach and not being put off by all the buzzwords and jargon.

"Risk Management continues to be inflicted with new interpretations. It has gone from 'holistic' to 'integrated' to 'enterprise', and one of the latest is 'intelligent' risk management. Fortunately, one description has vanished - 'boundary-less' risk management. They all mean the same thing, that is, all risks have to be managed," he says.

Williams' view is risk management needs to be addressed at a senior level within a company and there needs to be a single focus rather than having a variety of third or fourth level managers addressing specific risks in silos with no co-ordination.

"You need to develop a culture within a business so risk management is not something that sits on the side but is part of doing business," he says.

Transpower, the national grid owner and operator, is a good example of a company taking risk management seriously. It outlines its approach in its statement of corporate intent.

"Transpower recognises that managing risk is an essential and critical component of its business. The board actively considers the strategic risks faced by Transpower and ensures Transpower has in place a framework within which major business risks can be identified, assessed, managed and reported on. The risk assurance group maintains a register of key risks and the risk management actions to be taken in respect of those risks. This group also liaises with internal audit functions and other assurance

providers and reports to the board's audit and compliance committee on a bi-annual basis. Transpower's risk management policy is approved by the board and reviewed annually by the audit and compliance committee."

It's an approach endorsed by Caragata. He says a risk management culture has to permeate every level of a company, starting at the top with the board.

■ Anthony Davies is managing editor of *financialalert*.

## CHECKLIST

- The core business activities supporting the business goals are clearly defined and articulated.
- Internal and external assets and resources that the core business activity are dependent on are clearly recognised.
- The effect that disruption of these core business functions might have on achieving the business goals is well understood.
- Reliable business continuity or contingency plans exist to ensure unacceptable disruptions do not occur.
- The effect that quality impairment might have on achieving the business goals is well understood.
- Line managers accept and understand their responsibilities to manage those aspects of risk that might threaten the business goals which fall within their area of influence and control.
- Efforts required to protect the business goals from the effect of risk which would be otherwise unacceptable are efficiently resourced.
- Risks are considered and accounted for in the strategic planning processes.

Source: Patrick Caragata, *Business Early Warning Systems*. Butterworths, Wellington 1999.

## How well is your organisation managing risk?

Associate Membership of the New Zealand Society for Risk Management is helping many organisations manage risk more effectively. It will help yours too.

Associate Membership offers your organisation most of the benefits of individual membership, including access to:

- the latest international resources
- professional colleagues and leading experts
- professional development opportunities
- events and contacts in your region
- participation in special groups
- Members'-only resources at [www.risksociety.org.nz](http://www.risksociety.org.nz)
- the Society's newsletter.

The New Zealand Society For

**RISK MANAGEMENT Inc.**

[www.risksociety.org.nz](http://www.risksociety.org.nz) [executiveofficer@risksociety.org.nz](mailto:executiveofficer@risksociety.org.nz)