Would New Zealand Organisations Cope with Offensive Challenges to Continuity?

Dr Simon Ewing-Jarvie

Re-Print May 2014
(First Published February 2002)

In July 2000, Ian Laird and I published the findings of an initial survey (1000 organisations) into the state of business continuity planning in New Zealand. This was followed up with a range of interviews and a second organisational survey in 1999, which generated a substantial amount of data and many useful insights into the attitudes and behaviour of executives regarding continuity planning.

The events of September 11 in the United States have cast a spotlight on types of potential crises that, until that time, were not considered high priorities for many executives. These include events associated with offensive action taken by groups or individuals for motives ranging from business to political or personal reasons. The surveys conducted in 1998 and 1999 examined, in part, three categories of these events:

1. External economic attacks,
2. External information attacks, and
3. Psychopathology.

External Economic Attacks

The use of the term 'external' in this context means that people outside the organisation initiate the event. It includes extortion, bribery, boycotts and hostile takeovers. While NZ has generally been regarded as having low levels of corruption and hostile business practice, the increase in cross-border commercial activity – the 'global marketplace' - has no doubt caused an increase in risks of this sort. This was reflected in a July 1997 report by Transparency International that moved NZ from 1st to 4th place out of 52 in its Corruption Perception Index. No doubt, extensive media coverage of fraud allegations at the Audit Office, the Accident Compensation Corporation and the Inland Revenue Department (the latter referred to as the 'Wine Box Inquiry') has fuelled this change in ratings. There has also been an increase in reports or allegations of Asian Triad activity and staff bribery regarding waiting lists for Government housing assistance over the last decade.

Have New Zealand's executives taken this seriously and included it in their continuity plans? The latest data would suggest that they have not. In a series of YES/NO questions, respondents were asked what crises they planned to deal with. A 'YES' response scored a 1 and a 'NO' scored zero. From the sample, it is possible to establish the proportion of those in large organisations that plan for the following activities:

1. Extortion – 15% (out of 96 responses)
2. Bribery – 15% (out of 99 responses)
3. Boycotts – 16% (out of 97 responses)
4. Hostile Takeovers – 15% (out of 93 responses)

External Information Attacks

Closely linked to the first category is that of externally initiated information attacks. These include copyright infringement, loss or theft of information, counterfeiting and damaging rumours. The Copyright Act (1994), along with other statutes and case law governs intellectual property rights in NZ. However, it is limited in its application and duration of protection and the previous NZ Government indicated that it believes that aspects of the Copyright Act were contrary to the free trade principles espoused in the Commerce Act (1986) through the passage of a 1998 amendment that provides for the parallel importation of proprietary products. This has drawn criticism from many other countries and no doubt leaves the potential for self-justification of similar actions against NZ-made exports.

Hacking and cracking of computer systems has been well reported and the rapid uptake of networked systems in NZ makes this a matter of 'when' rather than 'if' it happens. While there have been a few successful prosecutions in the area of software piracy (counterfeiting), this problem is ongoing and threatens the development of NZ's fledgeling software industry. What then is the level of planning by executives in these areas?

1. Copyright infringement – 20% (out of 97 responses)
2. Loss of information – 64% (out of 102 responses)
3. Counterfeiting – 13% (out of 94 responses)
4. Damaging rumours – 43% (out of 100 responses)

Psychopathology

This category of hazard addresses abnormal or criminal behaviour by an individual or group against an organisation. It includes terrorism (both political and consumer), copycat behaviour, on and off-site sabotage or tampering, executive kidnapping and sexual harassment. Various researchers have observed that society is increasingly unstable and that, not only do problems spill over into the workplace but that they can affect the organisation's viability. Mentally unstable, aggrieved or jealous employees or ex-employees have, amongst other actions tampered with products, deliberately misapplied quality testing procedures and leaked sensitive corporate information to competitors, politicians or the media. Such actions are not limited to employees. A disgruntled customer filing a nuisance lawsuit or starting a petition might just as easily cause a crisis. Activists such as anti-vivisectionists or anti-abortionists have a single purpose in their campaigning and that is to modify or terminate the operation of an organisation. Politicians utilising parliamentary privilege can attack a company or pass legislation that can have the same effect. In the last decade, the media have reported equipment sabotage, arson, bomb scares in stores and food tampering affecting a wide range of NZ organisations. The survey results are as follows:

1. Terrorism – 24% (out of 100 responses)
2. Copycats – 5% (out of 94 responses)
3. On-site sabotage / tampering – 37% (out of 99 responses)
4. Off-site sabotage / tampering – 22% (out of 96 responses)
5. Executive kidnapping – 7% (out of 98 responses)
6. Sexual harassment – 79% (out of 102 responses).

The High Scores

In the article covering 1998 data, high usage was defined as scores of 75% or above. In 1999 the only event category that crossed this threshold was sexual harassment. This is not surprising given that NZ has comprehensive legislation requiring employers to actively protect staff against this contingency. While not strictly meeting the criteria described, planning against loss of information also scored highly at 64%. However, the interviews revealed that this may not only be a function of awareness of network vulnerabilities and the desirability of information security, but also a perceptual linkage with the need for data back-up.

The Low Scores

The criterion previously employed for identifying low scores was a result of 25% or lower. Clearly, all the remaining listed events, with the exception of on-site sabotage and damaging rumours fall below this threshold. Of particular concern are the results for copycat behaviour (5%) and executive kidnapping (7%). In addressing the question posed in the title, less than one quarter of large NZ organisations comprehensively plan to cope with offensive attacks on their continuity.

The Patterns

The 1999 sample has been further divided by type and size to see if there are any organisational patterns. In the table below, the first column shows the result for all organisations as given above. The private sector organisations are shown in the second column and the third column is the public sector result (comprising central and local government and the public health sector - excludes Defence and Police).

RISK EVENT	ALL	PRIVATE SECTOR	PUBLIC SECTOR
Extortion	15%	24%	10%
Bribery	15%	29%	8%
Boycotts	16%	23%	13%
Hostile take-overs	15%	28%	8%
Copyright infringement	20%	40%	8%
Loss of information	64%	69%	61%
Counterfeiting	13%	19%	10%
Damaging rumours	43%	46%	42%
Terrorism	24%	24%	26%
Copycats	5%	12%	2%
On-site sabotage	37%	43%	35%
Off-site sabotage	22%	31%	17%
Executive kidnapping	7%	14%	4%
Sexual harassment	79%	69%	85%

While a further breakdown is not possible in this short article, it is worth noting that, in addition to the mostly lower scores from the public sector, the local government result was clearly below that of the other two governmental divisions. Central government tended to score near the public sector median and the health sector was most aware of these events. Notwithstanding that, none of the three scored highly enough to change the overall result for each event.

In terms of organisational size, large organisations referred to in this article were subdivided into those with 100-500 staff and those with over 500 staff. In most areas, organisations with over 500 staff scored much higher than their mid-sized counterparts. The exceptions to this were, in the main, events in the area of psychopathology and interviews revealed that many executives from large organisations believed that their size was a defence in itself against this type of continuity challenge. The aftermath of the World Trade Centre is a sobering reminder of the fallibility of this argument.

Summary

The data shown here is only a brief snapshot of executive perceptions of these potential crises. However, it is useful in directing attention to future research activities and should serve as a reminder for NZ executives to recheck their assumptions in continuity planning. In particular, small to medium sized local government organisations appear to be particularly at risk. This is important given their role in maintaining essential services in all NZ communities.

For more information and free downloads visit our websites at:

http://www.torquepoint.co.nz
and
http://www.blackswans.co.nz