

Crisis management

Thinking beyond business continuity

Recent IT failures and data losses have focused the minds of senior managers on how to prevent such disasters and fix them quickly if they happen.

These same disasters, however, should also focus attention on much more strategic questions — how to minimise damage to reputation, how to ensure effective crisis communication that maintains proper messages and how to integrate potential IT risks into the broader context of corporate crisis preparedness and prevention.

Crisis management experts agree the greatest damage from a corporate crisis often comes not from the triggering event but from how the organisation responds — and the public perception of that response.

The key to effective crisis management is thinking beyond technical response to the triggering event. It is a particular challenge when it comes to IT problems, because of their inherently technical nature and the technical orientation of many IT managers. The truth is that IT crises are not just technical problems; they are often business, reputational and communications crises as well.

It is a reality that is amply demonstrated by two highly publicised recent Australian examples.

In September 2010, the electronic check-in system of Virgin Blue (now re-branded Virgin Australia) suffered a high profile crash which stranded thousands of travellers for

11 days. Faced with a major threat to its business and its reputation, Virgin stressed that the problem was another company's fault.

That may have been true, but was it the right strategic message to irate passengers? The airline also emphasised it had lost up to \$20 million and would pursue legal action against its contractor. Again, it was a message that might have pleased shareholders but provided little comfort to upset customers.

Indeed, when an out of court settlement with contractor Navitaire was eventually announced, it was once again Virgin's reputation which took a hit, not the IT service provider which nobody outside the industry had ever heard of.

Just weeks after the Virgin Blue crisis, NAB's funds transfer system collapsed, causing enormous — and totally predictable — media coverage and public outrage. Hundreds of thousands of people were unable to access their money and some areas of business virtually ground to a halt as the problem spread to other banks.

However, this major technical crisis was made worse by communication which appeared to lack a proper strategic overview. Media reports quoted the bank as saying the problem was almost fixed, but it wasn't. And the pain continued for days. We may not know exactly what happened behind the scenes, but it is a ▶



fair guess that overly optimistic IT engineers kept saying they almost had it licked, and the bank continued to relay that optimism unfiltered.

At the same time, the message leaked out that the entire fiasco had been caused by “one corrupted file”. Again, we don’t know what led to the release of that information. Perhaps it made sense to the systems experts. But to an angry public it served only to raise fresh concerns about competency and system design. How, the radio shock-jocks asked, could a single corrupt file bring down a major part of the entire banking system?

Regardless of what actually happened, it certainly affected the bank’s reputation. And it is a stark reminder that in good crisis communication, the messaging must be well planned and address the strategic needs of the whole organisation.

When NAB was struck by a similar funds transfer problem again in April this year, customers were just as badly impacted, but at least the messaging seemed to be more under control.

In any corporate crisis there are five basic things which must be done — right away.

- ① Apologise: We are really sorry for what has happened.
- ② Empathise: We do understand how you feel.
- ③ State the facts: This is the situation as we understand it.
- ④ Take action: This is what we are doing to deal with this.
- ⑤ Provide assurance: We are taking every step to help you and to prevent this happening again.

These steps may seem simple — and note that finding fault and assigning blame are not part of the initial formula — but putting them in place requires effective crisis leadership and commitment to a planned strategy.

Lack of planning and a strategy was certainly a hallmark of the now infamous US Veterans Affairs (VA) data loss in 2006, which is perhaps the mother of all IT security breaches. In that case a government data analyst took home a laptop and external hard drive containing unencrypted personal data about 26.5 million veterans and their spouses, including social security numbers and dates of birth.

The computer equipment was stolen in a burglary and the analyst immediately told the police and his supervisors at VA. It was a disaster of almost unthinkable proportions, made worse by poor management. Nobody told the Secretary for Veterans Affairs for almost two weeks, and another week passed before VA finally told the public.

In classic scapegoat fashion, the analyst was dismissed for a breach of protocol. But it soon came out that he had been taking this type of material home for years, with the knowledge and permission of his supervisors.

Such security failures are alarmingly common, but a massive IT failure or security breach is the nightmare of every CIO. The largest most recent incident occurred in April this year when Sony announced hackers had stolen the names, addresses and other personal data, potentially including credit card details, belonging to about 77 million people who have accounts on the Sony PlayStation Network, soon followed by further breach

Steps to support crisis management

What steps can an IT executive take to move beyond business continuity towards planned crisis prevention and crisis management?

- Support cross-functional analysis to identify and prioritise potential issues before they become crises.
- Work with other executives to help them understand the wider implications of IT vulnerabilities.
- Train staff to appreciate that a potential IT crisis is never ‘just an IT problem’.
- Recognise that when a IT crisis strikes the reputation of the whole enterprise is at risk.
- Ensure business continuity is fully integrated with corporate crisis planning.
- Actively combat silo thinking and the idea that ‘it’s an IT problem so let IT fix it’.
- Acknowledge that what makes sense to IT people can easily be misunderstood by others.
- Work co-operatively with communications professionals to ensure consistent and appropriate messaging when technical things go wrong.

None of this is particularly hard to do. It’s just a matter of setting priorities and getting on with the task.

involving another 24 million Sony accounts. At about the same time the Texas State Comptroller’s office admitted that personal details of more than 3.2 million citizens had been inadvertently posted on a publicly accessible website for nearly a year. The office sacked its head of innovation and technology, the head of information security and two other employees.

Business continuity is not crisis management

There can be a high personal cost, and strong and effective plans are needed to help an organisation deal with such failures and to ensure business continuity. But a business continuity plan is not a crisis management plan.

The single most effective method of crisis management is not just to deal with the triggering event and subsequent clean-up; it is taking positive action to help prevent a crisis happening in the first place.

It requires strategic planning and cross-functional co-operation and the direct personal involvement of top executives across the whole organisation. **CIO**

Dr Tony Jaques is the managing director of Issue Outcomes. He specialises in auditing corporate issue and crisis processes and helping organisations identify and prioritise potential crises. Contact him at tjaques@issueoutcomes.com.au

