Cybersecurity Takes Centre Stage As A Crisis Risk

By Dr Tony Jaques

2014 was a landmark year for cybersecurity, one which saw a real change in reputational risk for corporations and other organisations. It also reinforced once and for all that hackers and data breaches are never 'just an IT problem'.

The year began with US retailer Target admitting that hackers stole personal financial details of up to 70 million people in a pre-Christmas raid, and the World Economic Forum in Davos declaring cybersecurity a major global risk. The year ended with hackers compromising the details of 83 million accounts at JP Morgan Chase, making it one of the biggest data breaches in history, followed by the utter debacle of the Sony hacking attack, and North Korea threatening retaliation over a supposedly funny movie about the assassination of Kim Jong-Un.

2015 has not started much better, with hackers hitting the US military's Central Command Twitter and YouTube accounts, as well as hacking accounts at Delta, Twitter and Newsweek. The Pentagon decided to call their breaches an "annoying prank" and said they did not affect military networks and that no classified or operational data was accessed. Privately, however, they must have been very worried.

Of course, cybersecurity is nothing new. But recent events have helped moved the focus from firewalls, and criminal penalties, and technical solutions to corporate crisis response and reputation management. Organisations that are the victims of hackers are routinely criticised for poor online security, for failure to take proper measures, and for slow or inadequate communication to affected parties.

Moreover, the cyberattack on Sony and its decision to withdraw the movie *The Interview* in the face of North Korean threats moved cybersecurity onto front pages around the world and mobilised a new crowd of stakeholders and commentators, including film stars, free-speech advocates, and politicians right up to the White House. It is ironic that all of this attention should be generated by a movie which film critic Scott Mendleson called a "below average comedy" on his list of top ten most disappointing movies of the year.

While Sony eventually authorised a limited release of the film, a conga line of self-appointed experts attacked every aspect of the company's response – for giving in to threats, for potentially endangering the lives of moviegoers, for undermining free speech, and for making the movie in the first place.

Managers everywhere should take note that cybersecurity has now well and truly moved to centre stage as a crisis risk. It has always been true that how an organisation responds to a crisis can be a far greater risk than the crisis event itself and can endanger the reputation of the whole enterprise. As the Sony case shows, this is certainly true when it comes to a cyberattack.

The CEO of Sony admitted his company had "no playbook" for how to respond, but he argued that his firm was "adequately prepared" but "just not for an attack of this nature", which he said that no firm could have withstood. Maybe he deserves some sympathy, but the reality is that many organisations are still focussed mainly on technical solutions

It is easy to be critical after the event, but IT failures and cybersecurity breaches do not have to be a reputational disaster.

and are not prepared to manage a cybercrisis at a management level.

The threat is not confined to American corporate giants. A recent report showed that Asian countries are seen as the most likely targets of cyberattacks in the world, and a study of Australian small to medium businesses showed that more than half have no risk plans or strategies in place in the event of a crisis. In fact, it was an Australian IT disaster – the payment system crash at National Australia Bank (NAB) in November 2010 – that helped reinforce the crucial link between system security and corporate response and reputation. The crisis quickly spread across the finance sector and left millions without pay or social benefits, and no access to accounts, ATMs or EFTPOS.

Some of the bank's 'explanations' were most unhelpful, such as "the outage was caused by a corrupted file" and "someone in IT uploaded a faulty software code". Equally damaging to the company's reputation and credibility were the constantly changing predictions of when the problem would be fixed, that presumably came from over-optimistic IT engineers and were blindly accepted by corporate communicators. On day one, the time to sort out the disaster was "hopefully by later today", but two weeks later NAB was still reporting "some inconsistencies".

NAB even committed the elementary mistake of allowing its spokespersons to say, "These things are very rare. This is, hopefully, a one-off incident." Such statements are bound to backfire and, sure enough, the NAB payment system briefly crashed again less than two weeks later (9 December). Little wonder that Fairfax Business Reporter Chris Zappone concluded NAB had a reputation as "the most accident-prone of the major banks in Australia".

There were many contributing factors, but it is clear that a major factor was the failure to publicly demonstrate that top management was taking responsibility, and that this was much more than just a systems problem. In fact, the then CEO had no substantial media presence during the crisis, other than putting his name to a national apology advertisement published five days after his company's systems went down.

It is easy to be critical after the event, but IT failures and cybersecurity breaches do not have to be a reputational disaster. In February this year, American health insurer Anthem reported that personal information of 80 million of its clients – including social security numbers and credit card numbers – was exposed through a cyberattack. Moreover, reports indicated that Anthem failed to encrypt the personal data in its systems and that the breach was enabled through a simple password hack, made worse by its single-tiered access design of the network. At a technical and business level it was a disaster. But the company's response was a lesson in how to protect reputation. Anthem:

- self-discovered the breach and reported it to authorities
- publicly announced the crisis within days of the discovery
- provided extensive and coherent information and updates to the public
- communicated to all stakeholders in the form of an extraordinarily effective letter from the CEO

After clearly stating the facts and what the company was doing about it, CEO Joseph Swedish wrote, "Anthem's own associates' personal information – including my own – was accessed during this security breach. We join you in your concern and frustration and I assure you that we are working around the clock to do everything we can to further secure your data." He concluded, "I want to personally apologise to each of you for what has happened, as I know you expect us to protect your information. We will continue to do everything in our power to make our system security processes better and more secure, and hope we can earn back your trust and confidence."

Anthem justifiably won widespread praise for its response. But the case underscores one critical point. Cybersecurity clearly now rests firmly in the executive suite as a crisis risk and no manager has any excuse for thinking that it is 'just an IT problem'.

Dr Tony Jaques *is an internationally recognised authority on crisis and reputation. His Melbourne-based company specialises in best practice audits of issue and crisis processes (www.issueoutcomes.com.au). Tony writes Australia's only issue and crisis newsletter, Managing Outcomes, and is author of the new book* Issue and Crisis Management: Exploring Issues, Crises, Risk and Reputation *(Oxford University Press, Melbourne).*

Cybersecurity clearly now rests firmly in the executive suite as a crisis risk and no manager has any excuse for thinking that it is 'just an IT problem'.