We've had a data breach. Let's not tell anyone...

So you have had a data breach. Do you fix it and keep quiet? Or tell the world and risk the consequences? And should you disclose a breach if not legally obliged to? **Tony Jaques** discusses

A major fuel company was recently confronted with this challenge after a data breach. The way it responded and communicated its response provides a worrying lesson for crisis managers everywhere.

In November 2017 an unnamed person alerted New Zealand petrol company Z Energy that a critical flaw in its online fuel card system potentially exposed customer records, including names, vehicle registration details, where and when they bought petrol and, in some circumstances, even their home address. It was also claimed that with the click of a button, an intruder could suspend all online accounts. Moreover this was reportedly not a deliberate hack, but simply a fortuitous discovery.

Z Energy is a major player in the New Zealand market, where it is a listed public company that supplies about one third of the country's petrol. The Z Card Online site serves 45,000 cardholders and is used primarily by businesses to keep track of petrol accounts.

In response to the anonymous email, the company attempted a discreet system patch. However the same informant later contacted the company again, saying the so-called fix was "half baked" and that data was still vulnerable. Almost three weeks after the first contact, the company took the system down, telling customers it was dealing with a technical issue. It subsequently said the site was down because: "Our technology experts have been building a new online portal."

Data breach reporting is not yet mandatory in New Zealand and the company did not disclose the issue to the Stock Exchange or the Privacy Commissioner. Instead its 2018 annual report vaguely reported that unspecified 'operational failures and shortfalls' had adversely affected customers.

"We acknowledge these events made life and business tougher for our customers than it should have been. For all of that, we sincerely apologise. We've learned from it and taken actions. We responded to these issues with reviews akin to those typically conducted for a workplace fatality. That is how seriously we have taken our poor operational performance during that time," the report noted. The company also said it had upgraded its cyber security.

But, as Clare Boothe Luce once quipped: "No good deed goes unpunished." In June 2018, seven months after the initial report, and four months after the card system was reinstated, it all began to unravel.

The unnamed person decided to share the story with local online news service *Stuff Circuit*, which began its own inquiries and contacted Z Energy.

The company was seemingly unprepared for this obvious eventuality and its spokesperson's response was both disingenuous and unhelpful: "Yes, our Z Card Online system was taken down for a period while we made some improvements and changes. But it is now back up and running and we really don't have any more to add on this."

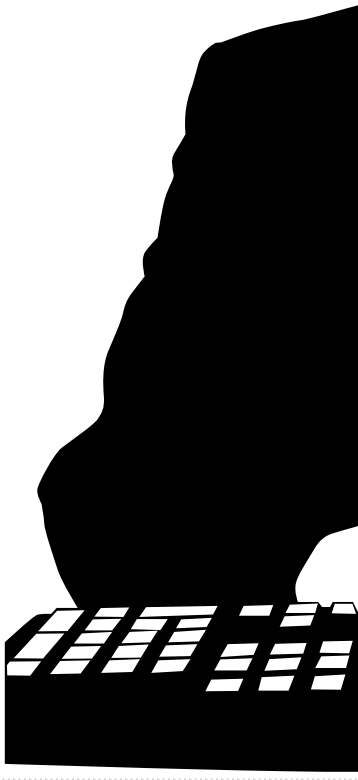
To say you have nothing more to add is a basic crisis response mistake that typically serves only to encourage further investigation. Needless to say, reporters at *Stuff Circuit* kept digging and in late June, Z Energy CEO Mike Bennetts sat down for a videotaped interview.

Bennetts seemed calm and well-rehearsed, with some clear, prepared messages. He explained how a system vulnerability had been identified in November 2017, but insisted experts found no evidence at the time that data had been compromised. Therefore, he argued, it was vulnerability, not a breach, and there was no need to tell customers. He said the steps taken were appropriate given what they knew then, and he followed up with some classic third party endorsement to spread responsibility, saying: "We took advice from outside parties, experts in this matter, as well as government agencies, about how to deal with this matter. And each step of the way, we were advised we were doing the right thing."

However, when presented on camera with a screenshot showing data from his own company's vehicle fleet account, he conceded: "It certainly is a security breach." And he agreed that in light of this new information, the earlier response had not been appropriate.

The whole case seemed to be captured in reporter Paula Penfold's final question on video. "Doesn't it seem extraordinary that you had a whole 'war room' and were consulting with all these experts, yet one member of the public was able to simply change an account number and a URL and get all this information?"

Bennetts replied: "Yes, certainly very, very disappointing and I apologise to our customers. As I said, sometimes these things happen and that is why we conduct independent and internal



checks to make sure we are constantly increasing things. This is something that was missed on the way through and we are very sorry about that." While the CEO generally handled the interview well, for him to say that these things happen hardly assisted a convincing apology or explanation.

On the basis of the 'new information' presented, Z Energy only then disclosed the breach to the market and the Privacy Commissioner.

Yet *Stuff Circuit* reported that a company spokesperson admitted the very same evidence had been emailed to the company by the original informant seven months earlier. The spokesperson somewhat naively said the email was received in "good faith" in the belief that the person would not share it with anyone else. The fact that this had been shared with the news media: "Changed the nature of the incident," and meant the company, "Chose to deal with this differently." This reveals the company's apparent failure to prepare for even the highly predictable risk of a leak to the media.

Astonishingly, the spokesperson went on to say the CEO did not know about the screenshot showing that the company's own data had been accessed until it was presented to him during the fateful video interview. The explanation offered was that: "He was out of the country at the time it was first given to the company."

Defending the company's actions, the spokesperson spelled out to *Stuff Circuit* that it did not want to keep quiet about the incident, but did so on advice. "We repeatedly challenged this counsel as it did not sit well with our values, but ultimately chose to follow the advice of our experts, given our commitment to cyber security."

Speaking of values, the CEO proudly told his interviewer about the corporate value he called: "Being straight up." This was formally described in the company's latest annual report: "We're committed to being straight up with journalists and the media. That means providing meaningful information, giving straight answers, and setting new standards of transparency in our industry."

Transparency

Sadly, the case of the Z Energy data breach gives little indication the company is setting standards of transparency. The most charitable interpretation of events is that the company tried to conceal an apparent data breach; failed to advise the regulator or shareholders in a timely fashion; created a misleading narrative for customers; seemingly didn't keep the CEO fully informed; had no effective media strategy; and finally came clean only when there was no other option.

In light of planned moves in the New Zealand Parliament to introduce mandatory reporting of data breaches, this is a salutary lesson to the company in question – and others – to get their act together. Quickly. CRJ

■ *The* Stuff Circuit *interview with Z Energy can be found at https://interactives.stuff.co.nz/2018/06/offline-z-energy/*

Nicolai Gergoriev | 123rf

To say you have nothing more to add is a basic crisis response mistake that typically serves only to encourage further investigation

Author

DR TONY JAQUES *is an internationally-recognised authority on issue and crisis management and Director of Melbourne-based Issue Outcomes Pty Ltd, which audits corporate issue and crisis management processes to help organisations identify and prioritise potential crises*