Wigley+Company solicitors

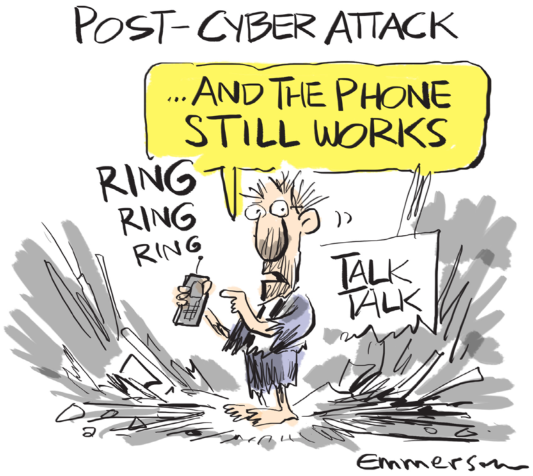
Cybersecurity silver linings in clouds for directors

March 2016

Speed read

In our January 31 article, *What should directors do about planning for a cyber breach?* on NBR ONLINE, we focused on the directors' role in the cyber breach crisis last quarter at UK Telco, TalkTalk. It's useful to look at what has happened since as it shows how a cybersecurity failure can be turned to wins.

This article was originally published in National Business Review.



The Detail:

Talk Talk's share price had tumbled due to the breach, and, now confirmed in the company's quarterly results, 95,000 customers were lost because of the hacking. Plus, the breach cost TalkTalk £60 million. The company had bad PR problems and did some things sub-optimally but the directors did some things right by at least having cybersecurity on the agenda every month up to the breach, plus three in-depth cybersecurity board sessions in 2015. Directors can't just tick the boxes like that to remove legal liability but it goes a long way, and probably gets directors off the legal hook even if the company is legally exposed.

That's a lot more focus than most New Zealand boards – by an order of magnitude.

Fast forward to last month's quarterly briefing to the market for the fourth quarter. Despite those problems, the brand is in fine shape as TalkTalk worked through the problems carefully.

Half a million customers took up a free upgrade offered as a retention sweetener by the telco. The briefing also confirmed that independent external research shows that customers perceived the company handled the problems honestly, openly and could be trusted, in the interests of the customers. So much so that the rating for honesty and trust is even higher than it was before the breach happened. As a challenger telco up against the incumbents like BT, TalkTalk is even pushing its branding overall as acting openly and honestly for customers against the bigger players. This goes to show how cybersecurity integrates with the broader picture, as it does with comms, HR, IT, legal.

So the TalkTalk CEO predicted a bright future financially. Quite a change from a few months earlier when some pundits predicted the company might collapse.

Another problem at TalkTalk

But TalkTalk will need to be careful not to have too many more incidents. As it happened, another problem did crop up

around the time of the fourth quarter briefing, although it hasn't caused too much grief for TalkTalk ... yet. What happened is that some customers – not many it's said

– who had visits to their homes by TalkTalk engineers, got followup calls from people who had full details of those visits. The caller got the customer to load TeamViewer on their computers, the customer of course thinking the caller was a genuine TalkTalk person. That's the sort of software most of us are familiar with that tech support use to fix problems remotely on our computers. The caller then tried to make financial transactions using the remote access.

Wipro, a major multi-national Indian outsourcing company, which provides services in New Zealand too, provides call centre services to TalkTalk and three of its India-based employees have been arrested in connection with this breach. This is an example of the importance, highlighted in earlier articles, of ensuring cybersecurity is sufficiently robust at the company's suppliers too. That's a legal issue for both the company and its board.

A new UK IOD cybersecurity report

On March 3, the UK Institute of Directors released its report, *Cybersecurity – Underpinning the economy*. A survey of business leaders showed they considered cybersecurity important but only 57% of their companies had a formal cybersecurity strategy. Only about 20% held cybersecurity insurance.

On planning for cyber-attacks, an inevitability, said the UK IOD report: *"As attacks become more prevalent and increasingly sophisticated, businesses need to defend themselves, know how to limit damage, and be ready to respond quickly and comprehensively when the inevitable happens. Boards should discuss how they would react to different scenarios and have a mitigation plan for when they are hacked or compromised. It is important that all departments are involved in this; cyber security is as much an HR issue as a technology one."*

Closer to home

According to Aura Information Security general manager Peter Bailey, it's not just international companies that should be putting cyber-risk on the agenda. The automation of attacks, the global nature of hacking and the ability of hackers to make cold hard cash out of their activities combine to make every business a target. It is therefore necessary for every company to prioritize information security and take reasonable measures to ensure safety.

Mr Bailey: *"Information security (InfoSec) should be a standard practice along with the many others necessary to run a good operation. The New Zealand IoD's Cyber-Risk Practice Guide provides a framework to help boards monitor cyber-risk, develop strategies for seeking assurance and to oversee management."*

Putting in appropriate security measures doesn't require the employment of highly trained specialists. Instead, companies and directors concerned about their security posture can do so by engaging with a specialist service providers.

We welcome your feedback on this article and any enquiries in relation to its contents. This article is intended to provide a summary of the material covered and does not constitute legal advice. We can provide specialist legal advice on the full range of matters contained in this article.