What should directors do about planning for a cyber breach?

March 2016

Speed read

Continuing our series on cybersecurity, we look at what directors should do about planning for cyber breach, and how what happened to a large UK telco, TalkTalk, late last year demonstrates the challenges for directors. This could happen to anyone.

This article first appeared in National Business Review.

Late in October, TalkTalk announced that up to 4 million customer details, including credit card information, may have been hacked (a few days later TalkTalk said that in the end this was limited to 156,000 customers).

The fallout for TalkTalk included:

- Share price dropped 27%.
- Loss of 7% of its broadband customers since the breach was reported.
- It came out that this was the second unrelated major breach in a year.
- TalkTalk announced remedial costs of £30M to £35M.
- The UK equivalent of the Privacy Commissioner criticised TalkTalk for not notifying it sooner. (Although the delay was only a few hours, it was talked up in the media and it's hard to avoid the impression that TalkTalk's transgressions were talked up overall, beyond the reality: but this is the real world in which companies have to operate).
- Press reports that scammers had phoned customers and, by pretending to be TalkTalk staff and leveraging off credit card details, persuaded them to part with large sums. (In fact the actual position may be that little has been lost but that didn't stop early days' press such as the widow whose husband recently died of cancer said to have been scammed out of £15,000).
- The company faced extremely difficult judgment calls in the first few hours on when to release information publicly, when the information on what had happened was sketchy and there were differing perspectives (for example, the Police asked them to defer announcing the breach).
- The ages of the UK based people arrested in relation to the hack are 15 to 20.

What should directors do about planning for a cyber breach?

- The Daily Telegraph and other media have focussed on the crisis and that's fuelled the problem for TalkTalk. For example, the Telegraph reported:

  "Several customers have come forward to say that TalkTalk ignored them after they rang the company in recent weeks to warn them that they had been contacted by suspected scammers.

  Paul Moore, an information security consultant with Urity group, said he had warned the telecoms giant about its security problems last September.

  TalkTalk had changed the way it processed credit and debit card payments, but it reportedly ignored his concerns about a lack of encryption.

  Mr Moore said usernames and passwords for email accounts were not encrypted, making them accessible to data breaches, despite the firm's chief executive's office assuring him that "we are squeaky clean on security".

  TalkTalk now admits that "more should have been done" and apologised for the "worry and frustration this attack has caused our customers".

And this happened where cybersecurity was a big issue for the board.

All that happened, even though cybersecurity was an item at every board meeting and that over the 9 months up to the breach, the board had three in-depth cybersecurity sessions. And that's a level of focus that is unusually high for a New Zealand board. By an order of magnitude.

That highlights that:

- There is no fool proof solution to cybersecurity;
- It will be important to make sure there is sufficient management focus on the right things instead of – as experts say happens too much – spinning wheels on the wrong things (one option but not the only one is for the board to get advice); and
- The board, by its documented attention to cybersecurity may avoid directors' liability: for the TalkTalk board, that may have eliminated directors' liabilities as to a company that some pundits thought might go under due to the cyber breach. Of course, every board wants to see their company prosper, but it's also right to take steps to protect themselves against personal liability. The by-product is that the company is less likely to have problems, for a mere going-through-the-motions approach won't get the board off the hook.

Planning for a cyber breach

When the CIO or a reporter phones the CEO or the Chair to say there's been a cyber breach, that's not a great time to learn how breaches work and what to do about them. Nor is it a good time for the company's internal people, and external advisers such as comms, legal and technical, to upskill in this area. They must hit the ground running, as a team.

Good plan. Good people. Reduce directors' legal exposure.

Directors' legal duties

Following our earlier conclusions in this series of articles, we consider the board probably has a legal duty to ensure the company has a robust cyber breach response plan in place. It's challenging for boards and senior managers to prioritise relative risks, when so many jostle for attention. But the fact is that the company is very likely to have cyber intrusions, the potential impact of some intrusions can be highly damaging to reputation, financial exposure and shareholder value, and

What should directors do about planning for a cyber breach?

execution of a good post-breach plan can make all the difference. That implies a legal duty on directors to ensure adequate plans are in place and the right people are in the team. This is well beyond flavour-of-the-month shroud waving.

For example, as the Australian equivalent of the Privacy Commissioner pointed out in October:

> *"All entities should have a data breach response plan. Your actions in the first 24 hours after discovering a data breach are often crucial to the success of your response. A quick response can substantially decrease the impact on the affected individuals."*

Talk to experts in the field and they'll say the same thing. Michael Wallmansberger, Chief Information Security Officer at Wynyard Group (who also has long governance and board experience) notes:

> *"Cyber incidents are analogous to fire. A well-drilled evacuation plan should prevent loss of life and serious injury if fire breaks out in a modern building. However, unless adequate fire suppression systems are in place and fire trucks are ready to respond, fire may still cause significant economic damage. In cyber security, a good plan will minimise the worst impacts, for example the damage to reputation that comes with appearing uncoordinated and ill prepared. However, a response plan cannot entirely compensate for inadequate protective security controls or limited response capability."*

Says Anna Kominik, a specialist in crisis comms, who facilitates courses for boards on how to manage reputation during crisis (and who presents the IOD's course on *Leading through a media crisis*):

> *"Be clear on roles and responsibilities, to connect the internal/business continuity with the external/ reputation management in a pressured and time poor environment, where companies and boards are often working with partial information. The plan needs to be kept up to date (for example, cyber security issues change frequently) and road tested.*
>
> *Four out of five business leaders expect their companies will experience a media crisis in the next year, but barely half have a plan to deal with it. Crisis can put board members in front of the media and the public in a way they never anticipated. The best advice to boards is 'have a plan', not just for cyber breaches, and make sure they've practiced it."*

The legal dimension

On the legal dimension, one of the five principles for boards in the Institute of Directors' cybersecurity guidance is to *"understand the legislative environment"*. We'd add that boards should understand the wider legal environment, such as contract and duties as to confidentiality, not just the legislative dimension.

The post-cyber breach plan should integrate the legal aspects, ready to be utilised in the urgent circumstances.

The legal defensive shield

As we outlined in our last article, *Five core principles*, we like the approach of the GC100, which is the association of general counsel and company secretaries working in the UK's FTSE 100 Companies. They have a legal model based on a *"defensive shield"* for the company, designed *"to protect an organisation from regulatory actions and litigation."* Essentially, the *"legal defensive shield"* would have the legal risks adequately assessed, and how to deal with those risks in terms of reducing risk worked up. This includes planning for the legal issues that crop up after a cyber breach. For example, planning for how to deal with

What should directors do about planning for a cyber breach?

insurers when urgent action must be taken. (On that topic, while cyber risk insurance is valuable, it is far from being a panacea, so companies and boards still have substantial steps to take).

Another example of a post-cyber breach legal issue is whether the company should tell affected people about the breach. (That raises challenging broader comms and reputation judgment calls too, of course). If New Zealand follows the way of many countries – Australia most recently - there will be a new Privacy Act provision requiring mandatory reporting to affected parties where a breach has significant impact. But arguably something like this applies already in some cases, as the Act currently provides that a company *"shall ensure … that the information is protected, by such security safeguards as it is reasonable in the circumstances to take, against loss … and…use"*. Take the TalkTalk scenario where credit card details were hacked. In New Zealand, that implies there might be a legal responsibility to notify the credit card holders so they can cancel the card details, so the information cannot be used by the hackers. This conclusion is not clear, although what is clear is that not mitigating damage by taking appropriate steps can lead to greater legal exposure.

Companies and their boards will have both legal considerations applicable to all, and then some industry specific legal concerns too. The TalkTalk scenario shows how challenging this can be for boards, but also it may be an example of how the board has – rightly – been able to protect itself, by its documented attention to cybersecurity.

- Part one: *Lessons for NZ boards in Juniper scare*
- Part two: *What John Greaves' predicament teaches us about cybersecurity obligations*
- Part three: *It could happen to you*
- Part four: *Five core principles*

Wigley+Company
PO Box 10842
Level6/23 Waring Taylor Street, Wellington
T +64(4) 472 3023 E info@wigleylaw.com
and in Auckland
T +64(9) 307 5957
www.wigleylaw.com