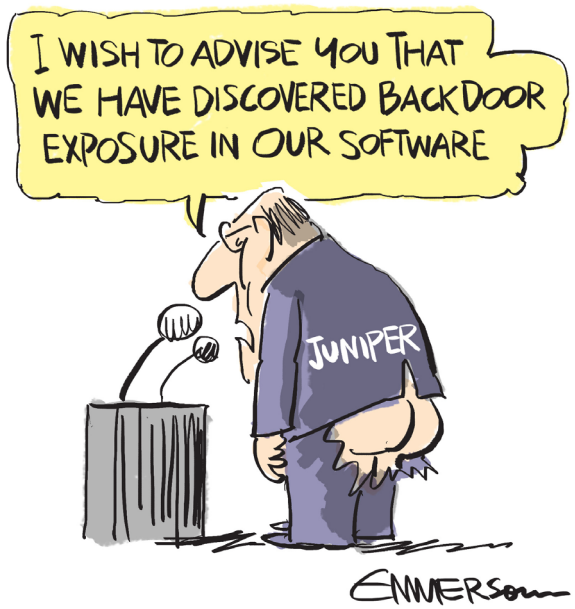
Lessons for NZ boards in Juniper scare

January 2016

Speed read

What is a company board to do when it emerges, as it did just before Christmas, that even highly robust and secure IT equipment and software, commonly in use in larger companies in New Zealand, is found to be insecure?

On 20 December, Juniper Networks, market leader along with Cisco in high-end networking equipment, issued an urgent notice to its customers to patch up a vulnerable "backdoor" in its firewall and router software. Plenty of NZ companies use Juniper, including telcos.



In this, the first of 5 articles originally published in *NBR*, we overview what this means for legal duties of directors as to cybersecurity.

The Detail

The Juniper problem

Essentially, knowledgeable hackers could access the organisation's firewall via a hardcoded password and decrypt encrypted traffic captured outside the organisation's network. They could potentially access the company's data and create other mayhem for the business, of the sort the Ashley Madison and Sony attacks illustrate.

As the urgent Juniper notice said in tech words:

> *"During a recent internal code review, Juniper discovered unauthorized code in ScreenOS that could allow a knowledgeable attacker to gain administrative access to NetScreen® devices and to decrypt VPN connections".*

Cisco has reported that it is doing its own urgent review in light of the Juniper announcement. Industry experts report that other major providers will be doing the same but that this is tip of iceberg territory. There is informed speculation that hackers have taken a "backdoor" in Juniper's software, crafted by United States spy agencies, and repurposed it for their own use.

What this says to directors

For directors, the Juniper problem, and other news in this area, highlights three key points to consider when deciding what to do about cybersecurity:

- Cybersecurity issues for the company extend beyond the company's own network. The company has major exposure via the company's suppliers' systems ranging from those of IT providers through to upstream supply chain providers and external consultants such as lawyers and

accountants (why waste time hacking into a company's robust network to get confidential information when it's held by the company's advisers under weak security?).

- If the highly secure and robust end of town has weaknesses, that says something about the range of risks when so many other risks exist of an inherently less secure nature such as employee use of smartphones.

- For all companies, cybersecurity is well established as a "bet the bank" risk, with a real prospect that, sooner than later, there will be a major breach. While companies and boards must realistically prioritise handling of various risks, and not be swayed by passing fads, cybersecurity should be right up the list. Says Graeme Neilson, Chief Research Officer at Red Shield Security:

  "Of the many penetration tests over 15 years I've been involved in for New Zealand organisations, there have been less than a handful where we haven't been able to access the client's system or sensitive data. My penetration testing colleagues tell me they have the same sort of experience".

There are enough war stories now to show that hackers can sink companies and/or destroy considerable shareholder value. It could be a hacker that doesn't like the company's moral approach (Ashley Madison). It could be the hacker is a foreign government that wants to stop the company doing something (Sony and the film on North Korea). It could be a disgruntled employee…. and so on. What is increasingly clear is that the potential range of attackers, and their underlying objectives, are so varied, that no company can say, "NIMBY".

Of course only some breaches and data entail "bet the bank" issues so a key step is to prioritise risks.

The focus for directors

The real issue for directors is not around whether there is a problem, but what does the board do about it. What we're hearing from experienced directors is along the following lines:

> *"Cybersecurity is right up there on the list of risks I need to be across as director: I've read enough in the news and heard enough to know that. But I can't quite get a handle on what I need to do to meet my duties as director. I am not sure for example, if I can leave it just to the CIO to reassure the board – with some detail from her - that cybersecurity is under control. I'm not sure how to handle this in the context of the other risks we manage, given we're here to make a profit too"*

In this commentary, the first of a series, I'll set out the legal starting point on how directors should deal with cybersecurity, although there are a couple of cautions:

- Cybersecurity is decidedly multi-disciplinary. There are strong IT, HR, legal, comms, sales/marketing, financial and other facets. While one person can be responsible – for example, larger corporates are increasingly appointing a Chief Information Security Officer (CISO) - the board would be wise to ensure there is a cross-company approach without siloes. Back in the day, when we were first involved in this area, the IT security people, typically buried deep within IT, did a great job but were frustrated as few seemed to listen: at least now it is recognised that there are major issues, involving multiple aspects of the business.

- As the legal cases are at pains to point out, the relevant directors' duties are fact specific for each situation. Of course that also means that a judge may take a different view of where the line is drawn in a director's negligence case, from what appeared to be right at the time. There can be a view among directors that the judgments unfairly impose higher duties with the benefit of hindsight. So directors should have a weather eye on what the courts might do.

What the law says

Like all other company risks, the law is clear enough in confirming that 100% cybersecurity is not required, as risk is to be managed and balanced with maximising shareholder returns. That is the "business judgment rule" in operation. Complete cybersecurity is not possible anyway, and going too far would probably make the company fail as business would be unworkable in practice, on top of the high cost. To illustrate, no company can afford to avoid grappling with the disruptive technology and the Internet of Things juggernauts, whether threat or opportunity, but those developments generally add to cybersecurity risk. So, there's a balance even though this is a "bet the bank" risk. The issue for the company is around how far to go in relation to cybersecurity for each category of data (and, in turn, what should the board do about that).

Directors know that their main relevant obligation under the Companies Act is to exercise the care, diligence and skill of a reasonable director in the circumstances, that they can delegate so long as that is reasonable, and so long as they reasonably monitor the delegation, and they can rely on company staff and advisers, and fellow directors, where that is reasonable. There are variations on the theme for executive and non-executive directors, for directors brought in for specialist expertise, for board committee members, and for chairs. The "reasonable" wording sets out an objective test. (There are other directors' duties too, including industry specific responsibilities, but we'll focus on this core requirement).

Companies with good corporate governance have robust board practices to manage risk to meet these duties, and what is clear is that cybersecurity should become well entrenched in regular board reviews, given the "bet the bank" risk and real prospect of successful attacks.

As Professor Watts says in New Zealand's leading legal text on directors' duties:

> *"While the business judgment rule looks to be, and is, of considerable comfort to those undertaking the role of director,.... the rule needs to be set against the fact that the courts have also required of directors a considerable degree of skill and diligence in their decision making. Even in relation to risk taking, which the business judgement rule is supposed to protect, [the judge, in a leading case] indicated that the greater the degree of known risk, the greater the degree of care that might need to be taken."*

That legal summary is, or should be, motherhood-and-apple-pie for directors, but it's as well to restate it, for, as to cybersecurity the 2015 Institute of Directors' Director Sentiment Survey reported:

> *"It is concerning that only 27% of boards are regularly discussing cyber risk and are*

confident about their company's capacity to respond to a cyber-attack or incident. A third are not confident and a further 40% are neutral/unsure."

I'll follow up with ideas around how far directors should go to meet their duties, including in relation to insurance and also as to DR prep for the day when and if there is a successful attack, for which careful multi-disciplinary planning is needed.

As the IOD survey recommends to directors, "Put cyber risk on the agenda before it becomes the agenda".

In Part Two, we will drill down into more detail on directors' obligations.

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