Most boards breach cybersecurity legal obligations

February 2016

Speed read

This is Part four in our series on cybersecurity and directors' duties.

In our second article, we outlined why we thought many boards would likely be in legal breach today if they weren't already implementing at least the IOD *Cyber-Risk Practice Guide* or similar. We now go into more detail, particularly around boards pragmatically handling this complex and fast moving area.

We summarise the Guide's requirements, set out some experience from the trenches, and then look at some detail from the perspective of directors, such as:

- How directors themselves can be a major cybersecurity weak point for their companies;
- Key management appointments such as the emerging role of the Chief Information Security Officer (CISO);
- The strategy and execution of a legal cybersecurity plan for boards: we call that the legal defensive shield;
- Some specific legal issues for directors.

This article first appeared in National Business Review.

Five core principles

The IOD guide has five core principles for boards:

- take a holistic approach on this enterprise-wide risk
- understand the legal environment
- access expertise and put cybersecurity on the board agenda
- establish an enterprise-wide framework
- categorise the risks

Context

First some context from the trenches. A standard magnitude of impact-frequency risk approach doesn't fit well for cybersecurity, says Graeme Neilson, chief research Officer at Red Shield Security:

> *"Attackers largely control likelihood (they determine how many resources to expend compromising the company) and impact (what happens when a compromise occurs is also determined by the attacker). Using pure risk assessment leaves lots of apparently low likelihood but high-impact cyber security risks on*

the risk register. Basically, compromises waiting to happen. Over many years, I have seen many companies with weak internal network security as a result of risk-based assessments. In my experience, an approach based on trust assessment and secure culture leads to a more robust security posture."

Michael Wallmannsberger, the chief information security officer (CISO) at Wynyard Group, with long experience also on boards, agrees and adds:

"The board needs to upskill itself, retain independent access to experts and/or appoint a board member that has security expertise, clearly define its security risk appetite, ensure that management assigns appropriate resources to an independent function to manage security risk, and hold management to account for risk. That takes more than asking a few questions, such as in the lists of questions in various guidelines."

Legal requirements

Companies are more likely to appoint experts in digital marketing, social media etc as directors ahead of those with cybersecurity credentials, so, while assigning cybersecurity responsibility to a committee makes sense, the board is likely to remain reliant on external advice. However, we think that, from a legal perspective, all directors will still need to have an understanding of the issues, updated sufficiently frequently, with cybersecurity on the board agenda sufficiently frequently. It's at the point that, just as an understanding of the financials cannot be left to the accountant directors, that is so too for cybersecurity.

Directors can be a cybersecurity weak point anyway

There's another reason why directors should upskill. A big part of cybersecurity is the people and culture aspects, so that all of the company's employees must be trained (for example, as to the use of their smart phones, use of passwords, etc). If a hacker wants to get a company's business plans and other sensitive material, why waste time attacking a relatively well-managed company network, when a director's home computer is more likely to have weaknesses unless careful steps are taken. Directors have many of the Crown jewels. Just like employees, if not more so, directors need training. A nice fit with board upskilling.

The CISO role

A key approach in reducing legal risk will be to make sure the manager responsible for cybersecurity is the right person, tasked with doing the right things, and is adequately resourced. Increasingly, there's a standalone role as CISO, outside the depths of the CIO's team where security people historically lived. Michael Wallmannsberger points to a JD for the CISO (or whatever else the role is called):

Working in security requires a certain mind-set (thinking like an attacker; non-linear thinking); the ability to apply a set of well-known (but not always well understood) security principles and patterns; a comprehensive understanding of the underlying technology that makes up the secure systems; and an ability to work across the business on multi-faceted issues including with the CEO and the CFO.

The CISO's job is to execute the strategy set by the CEO, within the risk appetite set by the board, within the budget set by the CFO. If the board's risk appetite is "conservative," the CEO's strategy is "once more unto the breach" and the CFO's budget is chump change, then the CISO – and the organisation – has a problem."

Simon Arcus, chief executive of the IOD, agrees CISO expertise will be critical for boards:

Most boards breach cybersecurity legal obligations

> *"We see the rise of the CIO or CISO role as the next big trend in boards as they come to rely on the company's technology knowledge base to make decisions. Pace is everything. We have an evolving cyber-threat to tackle. It is adaptable. Our cyber adversaries move with speed and stealth. Directors need to be conscious of contemporary risks and the need for a digital strategy to be on the agenda, and boards are now seeking executives with technology knowhow to help them better understand emerging cyber-risks."*

IOD's Principle 2: Boards must understand the cybersecurity legal environment

A core part of the company's cybersecurity duties is to understand the legal risks it faces. In turn, as the IOD guidance confirms, the board needs to understand this too (and also non-compliance can lead to board exposure; directors have been liable for negligence when that has led to a breach of company legal obligations).

The legal 'defensive shield'

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*."

Common legal issues

There are legal issues common to all companies. Obvious ones are the Companies Act and the Privacy Act. The core relevant obligation in the Privacy Act is that a company "*that holds personal information shall ensure –*

> *(a) that the information is protected, by such security safeguards as it is reasonable in the circumstances to take, against –*
>
> *(i) loss; and*
>
> *(ii) access, use, modification, or disclosure, except with the authority of the agency that holds the information; and*
>
> *(iii) other misuse.*

That fits nicely with directors' duties as, like those duties, it doesn't require 100% security but, instead, security that is reasonable in the circumstances (which varies according to sensitivity of data etc).

The act shows that responsibility remains when information is given to a third party (a big issue as we outlined in our first article):

> *" If it is necessary for the information to be given to a person in connection with the provision of a service to the [company], everything reasonably within the power of the [company] is done to prevent unauthorised use or unauthorised disclosure of the information."*

A less obvious example of a legal issue in a cybersecurity context is the new Health and Safety at Work Act 2015. The act includes mental health as well as physical. What if a staff member's personal details are hacked and publicised for example? Directors have due diligence obligations under the new act after it comes into force in April.

Industry-specific issues

Understanding specific acts and other law applicable to the particular company will be important and much will be situation specific. For example, cybersecurity issues may be material to directors' duties under the Financial Markets Conduct Act (for example as they may impact shareholder value).

And here's a trap as to the company's contracts, illustrated by this: A company may promise its customers that "*We will keep your information secure*" which is a legally enforceable 100% contractual commitment, quite different from "*We will take reasonable steps to keep your*

Most boards breach cybersecurity legal obligations

information secure." That is not to say the commitment is not made, but it better be made, knowing the risk given 100% security is not possible.

Cybersecurity will probably also have some international legal aspects for all companies but for some, even more so.

Next article

We will deal with what also is part of the directors' legal duties in our view: ensuring there is a crisis plan for managing the effect of a cyber breach. Typically this raises urgent issues. Not a good time for possums in headlights.

Part four in our series on cybersecurity and directors' duties.

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*

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