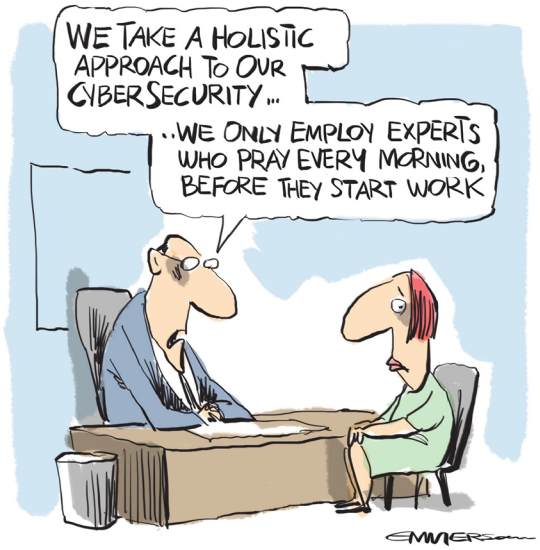
What John Greaves' predicament teaches us about cybersecurity obligations

January 2016

Speed read

In our first article in this series, we overviewed why cybersecurity raises legal obligations on directors. Using former board chair John Greaves' unhappy experience, we'll move to scoping the optimal approach for directors given (a) cybersecurity is a bet-the-bank issue involving fast moving complexities yet (b) the directors' need to be across the detail should be limited to what is required and delegated/ monitored appropriately, given the numerous other issues they must handle, not to mention the small matter that their main job is to build shareholder value and that rightly entails risk and trade-offs. Too much cybersecurity and the business dies.



If a board is not applying the Institute of Directors cybersecurity guidance – many aren't – it is not likely to be meeting directors' legal obligations

This article first appeared in National Business Review.

The Detail

What is enough, from a legal perspective?

We think the corporate governance and cybersecurity literature such as the Institute's *Cyber-Risk Practice Guide* will be particularly significant although there's more. We explain why many boards are probably in legal breach today if they aren't at least following guidance such as the IOD material, an unhappy place to be if there's a successful cyber-attack tomorrow.

Last year's *IOD member survey* indicates that it may be few boards are applying that standard. Given the ramifications of our legal view, we'll step through our thinking, using the judgment against Mr Greaves for alleged chairman's negligence to illustrate. He got stuck when such literature was effectively used against him. With cybersecurity, we have a new area with plenty of literature but little application by boards so far. The courts likely will look to the literature not the general board practice.

What John Greaves' predicament tells us

An Australian Judge assessed the standard of care expected of John Greaves, as chairman of ASX-listed One.tel, one of the more spectacular "tech wreck" failures in the early 2000s. The issues – around treatment of financials - were business as usual for directors. But we can then apply the conclusions to the emerging area of directors' responsibility for cybersecurity.

What John Greaves' predicament teaches us about cybersecurity obligations

Notably, the Judge is no slouch on directors' duties: he is the lead author of the top Australian legal texts on corporate governance and on company law. New Zealand and Australian law on directors' duties is similar.

It was claimed in the One.tel case was that the directors knew or should have known that particular events and transactions had the effect of unjustifiably improving the accounts so that the company looked healthier than it was. A common enough director's negligence story. One of the issues was the standard of care required of the chairman (with salutary conclusions for the duties of chairs). Included in the evidence put forward by the claimant to demonstrate the required standard were "relevant extracts from books, articles, and papers by learned commentators describing the customary responsibilities and the role of chairman…".

The judge concluded as to the chairman (but this is also applicable to all directors):

> *"Much of the literature of corporate governance is in the form of exhortations and voluntary codes of conduct, not suitable to constitute legal duties. It is sometimes vague and less than compelling, and must always be used with caution. Nevertheless, in my opinion this literature is relevant to the ascertainment of the responsibilities to which Mr Greaves was subject…".*

So far, so good (and the judge relied also on expert evidence from directors). Here's the most salutary part of the judgment on this issue, as Mr Greaves could end up being liable arising out of material he was not aware of:

> *"It may appear, at first blush, to be unduly harsh on a person in Mr Greaves' position that evidence of this kind might be relied upon to establish that in 2001 [when the breach is said to have taken place] he was subject to responsibilities and, ultimately, legal duties never before set out in a statute or by judicial decision. It should be remembered, however, that the Court's role, in determining the liability of a defendant for his conduct as company chairman, is to articulate and apply a standard of care that reflects contemporary community expectations."*

As noted in our earlier article, given each situation is fact specific, and that a judge's view, after the event, of what is an appropriate standard, and what are the "community expectations" (when creditors and shareholders are out of pocket), could be quite different to what some directors might think at the time. This point was firmly made by Jim Farmer QC, who represented the directors on the Lombard appeal (and he is also a very experienced company director), in September's Law Society seminar on directors' liabilities. As he noted, there is support for his view from the UK's senior appellate judge in a closely related and relevant area. Lord Neuberger said:

> *"We have to be very wary of relying on commercial common sense. First, a judge's idea of commercial common sense may be thought by some to be about as reliable as a businessman's idea of legal principle. Secondly, the judicial view of commercial common sense in a particular case is almost bound to be influenced by the facts as they have transpired since …., which should plainly be irrelevant to the exercise….".*

Add the likes of out of pocket suppliers and retiree investors to the mix, and all this indicates that directors should err on the side of a more careful approach but, importantly, that approach can in fact free up the directors and the company to take a more profit oriented stance (for example a paper trail for decision making is important).

What John Greaves' predicament teaches us about cybersecurity obligations

How does this apply to directors and cybersecurity?

When assessing the required standards of directors the usual starting point is expert evidence from other directors as to what is normal appropriate practice for directors. But in this emerging area of cybersecurity, and given the IOD survey – indicating only 27% of boards are regularly discussing cybersecurity - the court will likely instead look to what directors *should* be doing, not what they in fact are doing, in the context of the known issues and risks. We doubt that directors doing what many others are currently doing will get them off the hook when it comes to the present state of cybersecurity.

This is made even clearer by the directors' legal duty to keep on top of new developments. One of the leading judgments makes that clear enough:

> *"A director is obliged to obtain at least a general understanding of the business of the company and the effect that a changing economy may have on that business."*

And another judgment applied in New Zealand's leading negligence text says this:

> *"…where there is developing knowledge, he must keep reasonably abreast of it and not be too slow to apply it".*

As we outlined in our first article, if the board does little or nothing on cybersecurity, it is likely to be said by the court to be breaching its legal duty of care. (On all these issues there are arguments here and there, and each company differs, but this is a prudent conclusion. The same judge for example queried if directors' duties might be limited to purely financial issues, but it is not safe to rely on that and, anyway, cybersecurity squarely raises financial issues given companies can fail or there can be major loss of shareholder value).

So where does the court turn to figure out whether the director has met his or her duty as to the emerging cybersecurity area?

The cybersecurity and corporate governance literature likely will be a big start on this, for the reasons given by the Australian judge, so directors should ensure requirements – IT, legal, cyber threats, and so on - are proactively drawn to their attention, on a sufficiently frequent basis given so much change. But there's plenty of cybersecurity snake oil out there, and plenty of *"exhortation and voluntary codes of conduct, not suitable to constitute legal duties"* (although a judge's view on that after the event may differ from a contemporaneous directors' view). Key also is that the director is mainly there to enhance shareholder value and this inevitably involves risk taking.

The courts will also look at best practice such as what experienced external and internal cybersecurity specialists are saying: we are not saying the literature is the only source.

The minimum to meet legal obligations

The entry level approach for directors, to reduce legal risk, should be compliance either with the IOD's *2015 Cyber-Risk Practice Guide* or something at a similar level. When we've sued and defended directors for negligence, we've done the obvious thing of turning to the material put out by the directors' own professional bodies. It's compelling stuff for judges and no amount of legal analysis gets around the potency of that material in the real world. To ensure the IOD guide or similar is followed should be a legal "no brainer" for boards, particularly when the scale of the risk is now so well known, and that a competent lawyer for the claimants will tell the judge that the IOD is saying things to its members like *"It is concerning that only 27% of boards are regularly discussing cyber risk and are confident about their company's*

What John Greaves' predicament teaches us about cybersecurity obligations

capacity to respond to a cyber-attack or incident."

If one stands in the shoes of the Judge looking at this after the event, that is clear enough, well past shroud-waving and well past "the bloody lawyers being too risk averse".

We've noted that compliance with the IOD guide is the "entry level" approach. In our next article we'll explain why, and overview more specific steps boards can take, particularly to practically manage the scale of issues like this.

Part two in a five-part series on director's duties. Read part one, *"Lessons for NZ boards in Juniper scare"* here.

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