WannaCry ransom: what directors should do

June 2017

Speed read

The main takeaway from the recent WannaCry ransomware crisis is not that boards face cybersecurity challenges. Directors and executives already know this.

The real issue is: what should they do about it?

In this article, which reflects content from our new e-book, *Confronting cybsecurity in the boardroom*, we outline some key recommendations to help directors and executives deal with cyber risks and issues.

For example, boards should be looking to appoint a Chief Information Security Officer (CISO), and ensure that their cybersecurity plan includes wider input from finance, legal, IT, HR, and comms. Directors should also be aware that they don't have a legal duty to get right into the detail.

This article first appeared in the *National Business Review*.

Wigley & Company's new e-book, *Confronting cybersecurity in the boardroom*, is available on request. Please email info@wigleylaw.com for a complimentary copy.

The Detail

There's lots of shroud-waving going on at the moment from advisers, along the lines of: "*Heck, Joanne Director. WannaCry tells you to sort out your company's cybersecurity*".

But that really tells us nothing. The fact that companies and directors are exposed is not news.

Directors understand they have duties including legal duties as to cybersecurity, and, as shown by surveys such as the IOD's, many boards and companies fall short. They know too this is a big dollar and reputational risk, and that there will be plenty more variants on the WannaCry saga coming up.

The real issue is: what does the board do about cybersecurity?

The challenge here is that the board has a day job, and it cannot get too far involved in the detail.

A couple of things emerge from WannaCry that are significant for directors:

- Large organisations with multiple computer systems and many staff are particularly vulnerable (although much of that happened in the health sector, which cybersecurity experts rate as particularly exposed).
- Experts still aren't sure how the attack was done. The ransom may not have entered systems in the most prevalent way: by staff clicking on a dodgy email. This talks to the point that companies need to take a wide-ranging approach to cybersecurity as attacks can come from left field.

WannaCry ransom: what directors should do

While we've set out some detail on what directors should do in our new e-book, *Confronting cybersecurity in the boardroom*, co-authored with cybersecurity and comms/PR experts, here's some high level points for directors to watch out for:

- First, beware check-lists like this one! As Michael Wallmansberger, my co-author who is a cybersecurity specialist and experienced director, points out:

  "*There's a danger in a silver bullet approach as there are so many things to do, right across the business, to ensure optimal cybersecurity.*"

- The board doesn't have a legal duty to get right into the detail.
- Of course, the nicely written up cybersecurity plan the board ensures is in place needs to be backed up by the multiple business units and owners walking the talk, including updating the plan as things change. This includes ensuring cybersecurity is a regular feature on the board agenda and that the company's protections are tested. The plan needs finance, legal, IT, HR, comms and other input. It's a teamwork thing.
- To coordinate and manage all this, look at ensuring the appointment of a Chief Information Security Officer (CISO) or similar (in smaller companies, possibly as part of another role). There are external services too that provide similar support. Directors understand already that cybersecurity is not just for the CIO. Good CISOs have particular skill sets, including smarts to read the horizon and second guess where attacks might come from, given the particular risk profile of the company. Plus, they have skills in working across multiple managers and business units.
- Ensure a plan is in place for when there is a successful attack on the company. This includes not only IT but other aspects too, such as legal, comms and PR. The role of the board and the Chair should be included. All this can be integrated with broader comms strategies. When an attack happens is no time to be winging it. As Anna Kominik, my co-author and comms specialist, notes:

  "*A prepared organisation will have an established and tested crisis management plan, including a checklist for the first three news cycles (usually 6 hours, 12 hours and 24 hours after a crisis).*"

- There's a budgetary constraint theme that emerges among those focussing on cybersecurity in companies. We often see and hear that there isn't enough funding allocated to cybersecurity to sufficiently protect the company. Of course, that all involves the financial challenges faced by companies in allocating priorities. If budget means that the protection is lower, at least boards need to make an informed decision on taking that risk. There are trade offs.

That last point highlights that this is not an easy area for boards and senior managers to get right, where an attack could be quite serious for the company.

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