Wigley+Company solicitors

# Harvard Business Review: Cyber security is a bigger GC, board, CEO, and CFO issue

### Speed read

WE'RE UPPING THE ANTE ON CYBER SECURITY. FROM NOW ON, EVERYONE WILL BE USING ONE OF THESE...
SONY
TYPEWRITER
EMMERSON

There are valuable insights in the 24 March Harvard Business Review article, *See Your Company Through the Eyes of a Hacker*, around the role of boards, CEOs and other senior managers as to cyber-security.

It's not enough to just leave it to the CIO or to security specialists deep in IT departments.

The HBR article concludes that cyber security efforts have largely failed, requiring a change of direction using the military strategy of "*turning the map around*" (ie look at this from the perspective of the hacker).

There's plenty of sign that cyber security is a big risk issue for corporates, given widespread news ranging from the Sony Pictures hack, the Target hack (both Sony and Target CEOs lost their jobs) to Snowden revelations.

Exposure ranges from reputational and legal (eg hacking of customers' confidential details) to competitors taking IP such as CRM details and proprietary processes. Risk continues to escalate: for example, the Privacy Commissioner has recently moved to a name and shame approach for wayward entities causing data breaches, as we reported here. All IT security experts say that what happened to the Sonys and Targets of this world can easily happen to others too.

This is an edited version of our article that first appeared in the *National Business Review* on 17 April 2015.

May 2015

### The Detail

The Sony Pictures attack was a turning point because, until then, the very large breaches were financially motivated (stealing credit cards or bank account takeover, for example) or had obvious nation-state motives.

Sony Pictures demonstrated what can happen when an attacker just wants to burn you to the ground.

The hacked data included personal information about Sony employees and their families, e-mails between employees (some were extremely damaging to Sony and senior managers), copies of unreleased Sony films, and other information. While demands to cancel release of *The Interview* led to the FBI saying that the attack was driven by North Korea, experts have cast doubt on the evidence on this, proposing, for example, that current or former Sony Pictures employees may have been involved.

Highly respected US cyber security expert, Bruce Schneier, wrote in *The Atlantic* that he is "deeply skeptical" of FBI's position that North Korea is behind the hack as the evidence is "tenuous". Having listed other options, but not ruling out North Korea, he also noted more Machiavellian speculation by other experts. One says it's a smart strategy for the US Government to blame the North Koreans anyway, to discourage future hacking by other states. And he quotes a Harvard law professor, pointing to the vested interest of Sony in the hacker being North Korea: this could give immunity from law suits, as this can be characterised as an act of terrorism or war, or the work of a foreign power.

Either way, Sony is a poster child for the risks faced by all corporates, whatever the motivation. Most companies will have someone out there who wants to do damage: for financial gain; for revenge; or whatever. And they can be current or former insiders.

But our experience is that these issues remain largely covered only by IT specialists in the depths of IT departments, with little input or support from senior managers beyond CIOs. The risk, which is bet-the-bank stuff, is big enough to get the direct attention of boards, CEOs, CFOs and General Counsel, as we outlined in our article, *Top 100 General Counsel position on cyber security law and practice*.

That limited role of boards and senior managers in cyber security would reflect what many IT security people say. Boards and senior managers know about the risk – how could they not given the coverage – but don't engage enough. Here's what one NZ IT security specialist told me:

> *"The engagement (or more typically lack of) between IT security advisors and executive management is problematic for companies. For every CIO out there saying security is hard there's usually an expert working in his or her organisation that isn't being brought to the table. I spoke to a guy recently who had been doing the rounds of large company boards in Australia. He was asking directors if they realised they were on the hook for this cyber stuff. They said, of course we do: we take the advice of our CIO and he says we're fine. They're not fine, of course, but no large company CIO is going to walk into an executive meeting let alone a board meeting and say anything other than "we're golden"."*

HBR points out, when suggesting that companies should make security part of their mission:

> *"The prevailing approach to security is compliance-focused, cost-constrained, peripheral to the core business, and delegatable by C-suite leaders. Working on a team like that isn't fun inside any enterprise, and it loses against 21st-century adversaries who know that it's more fun to be a pirate than to join the Navy. Any defense is only as good as the people doing the defending. The new model of security needs to be about mission and leadership, ensuring that we have the best defenders up against the best attackers. Security is no longer delegable, and the mission of security teams must be synonymous with the mission of the company."*

The HBR piece has some great tips for Boards and senior managers.

The article's focus on "*turning the map around*" applies the military strategy of getting inside the mind of the enemy, to see the situation as they do, in order to prepare for what is to come.

For example, companies tend to focus IT security in limited ways, says the article, opening up ways around the sides.

The "*turning the map around*" focus would include, in the words of the article (but explained there in much more detail):

- Understand your major risks and how adversaries aim to exploit them
- Take inventory of your assets and monitor them continuously.
- Make security a part of your mission.
- Be active, not passive, in hunting adversaries on your network and removing them.

*We welcome your feedback on this article and any enquiries in relation to its contents. This article is intended to provide a summary of the material covered and does not constitute legal advice. We can provide specialist legal advice on the full range of matters contained in this article.*