Panama Papers: Legal implications for your organisation's cybersecurity

May 2016

Speed Read

The law is an important facet of the multi-disciplinary approach required to manage an organisation's cybersecurity risk. The Panama Papers hack at law firm, Mossack Fonseca, illustrates two points from a legal perspective.

The Detail

Law firms can be a weak point

First, organisation's law firms – of which Mossack Fonseca is an example but it's far from isolated – can be a soft target to hack into instead of the organisation. Lawyers typically hold valuable crown jewel type of information. Why waste time trying to crack into the organisation when the organisation's law firm less securely holds the information? The Panama Papers illustrate this so well, with their huge reach across hundreds of thousands of the law firm's clients.

Last month, for example, the major New York commercial law firms, Cravaths and Weil Gotschal, reported that they had been hacked. They handle some of the biggest US M&A transactions, litigation, etc.

There are insider trading opportunities for hackers on top of numerous other ways they can use highly sensitive information held by law firms.

But there are plenty more law firms on top of that being hit. In the last few weeks for example, we've learned of these New Zealand incidents (and this is just the tip of the iceberg):

- A sizeable law firm being held to ransom by cyber attackers, and they paid the ransom by bitcoin: and
- A phishing email which led the finance manager at a large law firm to pay funds to a hacker, based on an apparent email from the managing partner directing her to do so.

Law firms may have weaker cybersecurity than their client organisations, making them a prime target, given the valuable information they hold. As former head of the FBI's cyber branch in New York, Austin Berglas, recently told The American Lawyer, *"law firms are traditionally understaffed in cybersecurity, compared with large corporations and banks."*

Large organisations increasingly recognise this problem and some require stronger defences by law firms. For example, Bloomberg has reported that *"Many Wall Street banks, including Bank of America and Merrill Lynch, typically require law firms to fill out up to 20-page questionnaires about their threat detection and network security systems. Some clients are even sending their own security auditors into firms for interviews and inspections."*

Organisations have legal responsibility as to their information held by third parties

The second point is that many countries put legal duties on organisations to take steps to ensure that their information held by third parties such as suppliers is not placed at undue risk of being hacked. The organisation can't just rely on the third party (such as the law firms) to ensure it takes the right steps.

For example, New Zealand's data protection regulation – the Privacy Act - requires that *"everything reasonably within the power of the [organisation] is done to prevent unauthorised use or unauthorised disclosure of the information."*

Many of the cyberattacks involving organisations have been made via third parties such as suppliers that are associated with the organisation which is the ultimate target, instead of directly against the organisation.

So the legal duties as to the organisations' suppliers and other third parties are particularly significant.

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