Your law firm is vulnerable: Panama Papers hack shows how to easily steal companies' data

July 2016

Speed Read

Here's Fiona Campbell, formerly a lawyer with us but now working in corporate law in London, when passing through Panama City on her holidays.

This article was originally published in the *National Business Review.*

The Detail

The Panama Papers hack at law firm Mossack Fonseca illustrates four vital points for the company clients of law firms and their directors:

- Law firms are a prime target for attacking their client organisations (and it is happening here in New Zealand).
- In turn, those organisations have some legal responsibility for ensuring their suppliers such as law firms have adequate cybersecurity.
- Mossack Fonseca's cybersecurity vulnerabilities overlap with many that New Zealand law firms might have, meaning that their clients indirectly have those vulnerabilities too.
- Law firms' client companies often use the same sort of systems and software that Mossack Fonseca used, so this is a heads-up for the company's own security as well.

Law firms can be a weak point for their clients

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. As the Law Society of England and Wales notes, *"law firms are particularly attractive sources 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 many thousands of the law firm's clients. The hackers would get only a fraction of the information by targeting the clients directly.

We outline some of the cybersecurity weaknesses at Mossack Fonseca (weaknesses that many New Zealand law firms will have too), and the implications for New Zealand companies and their directors.

Your law firm is vulnerable: Panama Papers hack shows how to easily steal companies' data

In March, the major New York commercial law firms Cravaths and Weil Gotschal, reported that they had been hacked (as had many other major US law firms). They handle some of the biggest US M&A transactions, litigation and commercial work.

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

The range of hackers is wide and it's not just Russian criminals and the like: the latest major cyber-attack in the UK – the TalkTalk hack – was done by a handful of savvy English teenagers, for example.

There are plenty more law firms on top of that being hit. In the past few weeks 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 it paid the ransom by bitcoin; and
- a fake email from the law firm's managing partner, which led the finance manager at a large law firm to pay funds to a hacker. This is a variant on "social engineering" as a means of cyber-attack, and dealing with social engineering (by staff training, for example) is an important facet of cybersecurity.

Law firms often have weaker cybersecurity than their client organisations, making them a prime target, given the valuable information they hold. As a 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."*

What big corporates are doing about this risk

Large organisations are increasingly recognising this problem and some require stronger defences by law firms. For example, Bloomberg has reported: *"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."*

Illustrating that dealing with cybersecurity requires teamwork across multiple disciplines – such as ICT, HR, communications, finance, and legal – we asked some experts to comment. First is Michael Wallmannsberger, chief information security officer (CISO) at Wynyard Group: the CISO role is an increasingly important one in organisations and cybersecurity is central.

Michael Walmannsberger notes that maintaining rigorous internal cybersecurity policies is one of the best methods of ensuring third party suppliers are implementing similarly strong security practices:

> *"Information security audit by specialists is one of three foundations of security, without which little else matters. The other two are having clear policies on information security and knowing what IT and information assets your organisation has. There are many other important controls too but they will be ineffective without these three things.*
>
> *Internal audit, which is about checking that you are complying with your own policy, is necessary to achieve consistent security. It is also an excellent way to communicate to a range of business stakeholders what they are required to do to maintain security for the organisation."*

Your law firm is vulnerable: Panama Papers hack shows how to easily steal companies' data

Companies and directors have legal responsibility as to the companies' information held by third parties

The second point is that there are legal duties on organisations to take steps to ensure that their information held by third party suppliers is not placed at undue risk of being hacked.

An organisation can't just rely on a third party (such as a law firm) to ensure it takes the right steps. For example, the Privacy Act, at IPP5, requires that *"everything reasonably within the power of the [organisation] is done to prevent unauthorised use or unauthorised disclosure of the information."* There are many other legal obligations in this area, beyond the Privacy Act, and sometimes there are absolute obligations to protect data, not just obligations such as to take reasonable steps.

Directors' obligations in this area are particularly acute. We wrote a series of articles earlier this year in NBR explaining how directors' legal duties and their required standard of care extends to bet-the-bank issues like cybersecurity. By failing to implement industry best practice, such as the Institute of Directors' Cyber-Risk Practice Guide or similar, we concluded most New Zealand boards are in breach of their legal obligations.

Key requirements of the IOD's guidance material includes directors understanding the cybersecurity legislative environment and ensuring the implementation of enterprise-wide cybersecurity frameworks. Given that many high-profile cyber-attacks have been made via third parties associated with the organisation which is the ultimate target, instead of directly against the organisation, a robust cybersecurity framework must address third party risk.

The cyber vulnerability of suppliers and other third parties is an issue that must be dealt with by companies and directors to achieve legal compliance.

What cybersecurity failure led to the Mossack Fonseca breach?

Thirdly, there's how Mossack Fonseca was hacked. That's not known yet, at least outside Mossack Fonseca. It might have been an inside job but that is still a cybersecurity issue.

However, IT experts have been able to show many ways in which the attack could have been facilitated by Mossack Fonseca weaknesses. Many New Zealand law firms will have similar (or the same) applications and problems. Mossack Fonseca is not an outlier by any means.

The big issue for companies and directors is that if a law firm has these weaknesses, then the law firm's client organisations will indirectly share these vulnerabilities too.

Continuing the focus on inter-disciplinary expertise and teamwork, which I think is so important in this area, I sought advice from Peter Bailey, GM at Aura Information Security, a specialist cybersecurity firm that does, among other things, the cybersecurity risk audits which are best practice for organisations. This includes penetration testing, the process by which Aura takes steps such as trying to hack into the organisation, such as through firewalls and by social engineering.

Says Peter Bailey:

> *"It seems that Mossack Fonseca was running extremely out of date software. One of the means the perpetrators could have used to gain entry from an external starting point into the internal network was through a vulnerability in the website that could be three years out of date. It appears that the problem is systemic and that the infrastructure was riddled with critically out-of-date software.*
>
> *If you put a server on the internet, it will be attacked. Full Stop."*

Your law firm is vulnerable: Panama Papers hack shows how to easily steal companies' data

Here's an example of how this problem arises. Many law firms have content management software. Mossack Fonseca uses Drupal, which is a widely used open source programme (that is, freely available software that isn't proprietary such as Microsoft using software code; it is available for free to all programmers). Open source is a major part of many apps used by law firms, including some proprietary software, and it is a big part of cybersecurity risk.

Directors and managers will be familiar with the patches that pop up frequently on their computers to update proprietary software such as Microsoft and Acrobat. Or the computer informs the user that the updates have been done automatically (hence the frequent pop-up notice requiring rebooting). Often these fix security vulnerabilities on top of improving functionality. The fact that users are reminded to do the updates via the pop-up makes it much more likely that the vulnerabilities to attack are minimised. Open source software generally doesn't send out automatic updates to fix security vulnerabilities. Law firms have to proactively add the patches, as do their clients.

Where this doesn't happen – it didn't at Mossack Fonseca – the law firm can have a significant vulnerability to attack. For example, Mossack Fonseca's version of Drupal had at least 25 security vulnerabilities, known about since 2013 and for which there were patches.

Here's what Forbes said when reporting on the Panama Papers breach:

> *Back in 2014, Drupal warned of a swathe of attacks on websites based on its code, telling users that anyone running anything below version 7.32 [which is the version that Mossack Fonseca used] within seven hours of its release should have assumed they'd been hacked.*

As we note above, Mossack Fonseca is far from being an outlier. This is the sort of failing that penetration testing and regular cybersecurity checks are designed to uncover. As Peter Bailey says:

> *"This is a common problem for companies and one we often see when we penetration test websites for a number of organisations, both small and large. Again, regular security testing of your system is important, to look for any other gaps, flaws or even incorrect settings."*

Moving to another problem at Mossack Fonseca, Mr Bailey notes their poorly architected and implemented network infrastructure:

> *"The security of your network infrastructure is incredibly important – ensuring you have the right hardware and software in place to adequately protect your information. In this case, it was reported that possibly the Mossack Fonseca server was not behind a firewall. It is baffling why that is so, since having a firewall in front of an organisation network is pretty much standard everywhere else.*
>
> *A properly configured firewall provides a good degree of security on your network. A set of predetermined security rules runs in the firewall, and monitors and controls incoming and outgoing traffic. If anything looks like it doesn't belong, based on the rules, then it will be blocked. If you are not using a firewall on your own network, then you are opening yourself up to a number of network attacks."*

Another apparent vulnerability at Mossack Fonseca is what appears to be the absence of data loss protection (DLP) software. DLP detects potential data breaches and

Your law firm is vulnerable: Panama Papers hack shows how to easily steal companies' data

abnormal transmissions and prevents them by monitoring, detecting and blocking sensitive data and transmissions. While it won't always work, the massive amount of data being taken here may well have triggered a DLP to block its removal.

In summary, Peter Bailey observes:

> *Truth be told, security implementation is not easy. There are often so many various elements to consider and so many assets to protect. Weakness in any of them would potentially result in a breach. Consider engaging professionals to conduct a regular penetration testing to probe and evaluate the current implementation to identify gaps and weaknesses that might otherwise not be obvious to the organisation.*

The cost of inaction and third-party cybersecurity risk

The Panama Papers fallout provides a glimpse of what can happen when organisations are compromised through the cyber vulnerabilities of associated third parties, such as law firms, suppliers, and potentially even their own directors. Given that organisations are increasingly recognising (and are legally obliged to address) the issue of third party cybersecurity, the experience of Mossack Fonseca provides a powerful wake-up call for companies and directors in New Zealand.

The final word goes to Peter Bailey:

> *Here's some food for thought:*
>
> *Security is costly. But can you afford not to?"*

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