PANAMA PAPERS 101 FOR EMPLOYMENT LAWYERS

December 2016

The Panama Papers hack at law firm Mossack Fonseca illustrates that law firms can be a soft target for hackers to access Crown Jewel-type information held on behalf of their clients. In this conference paper we discuss why NZ law firms face similar cybersecurity exposure, and why this exposure is relevant not only for lawyers, but also for the companies and directors retaining their services.

Below, we explain that many NZ law firms are just as vulnerable as Mossack Fonseca to cyber hacks, outline companies' legal responsibilities towards ensuring that confidential information is protected by third parties (such as law firms), and highlight what big corporates overseas are doing to combat these risks. An effective response will likely require a multi-disciplinary approach to cybersecurity, "turning the map around" to think like a hacker, and preparing a comprehensive cyber breach response plan.

This conference paper was presented by Michael Wigley at the NZLS CLE Employment Law Conference, October 2016. Read the full conference paper below.

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

PANAMA PAPERS 101 FOR EMPLOYMENT LAWYERS

PANAMA PAPERS 101 FOR EMPLOYMENT LAWYERS

Michael Wigley
Wigley and Company
Wellington

The Problem for Law Firms

Cyber-attacks on NZ law firms are real. Here are New Zealand examples from the last few months. They are far from isolated:

- A sizeable law firm being held to ransom by cyber attackers, and it paid the ransom by bitcoin;
- A fake email masquerading as sent by a large law firm's managing partner, which led the finance manager at the law firm to pay funds to a hacker. This is a variant on "social engineering" as a means of cyber-attack. Dealing with social engineering (by staff training, for example) is an important facet of cybersecurity.
- A hacker getting into a law firm's internal system, ending up with a bogus internal email instruction from a partner to accounts to send client money in the firm's trust account to the hacker's account. Several hundred thousand dollars of client money was lost by the client.

The law firm at the centre of the Panama Papers illustrates another risk for NZ law firms: attackers getting sensitive information about clients because it is easier to get it that way than by going direct to the client. Plus, hacking in just one place – the law firm - can release a treasure trove about numerous clients.

About this Paper

We deal with the issues in this order, complementing Hamish Kynaston's paper:

- Panama Papers, and international experience: what does it tell NZ law firms?
- Why the law firm in the Panama Papers has the same sort of software and exposure that many Kiwi law firms have (it's a good case study);
- Legal issues as to cybersecurity for law firms (this is a good case study too for advising our clients on legal risk);
- What our clients are legally required to do as to their information held by us;
- Being prepared for managing the fall-out from a cyber-breach (it's not a great time to be a possum in headlights without having planned).

Panama Papers – it could happen to you

The Panama Papers hack at law firm Mossack Fonseca illustrates vital points for law firms.

What happened to the law firm in the Panama Papers case, Mossack Fonseca, also shows that attackers can get at the law firm's clients via the law firm.

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.

Below, we outline some of the cybersecurity weaknesses at Mossack Fonseca (weaknesses that many New Zealand law firms will have too).

International Experience

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.

US and UK data shows a fair bit of activity, as IT industry reporter, The Register, outlines in its 16 April 2015 article, *Miscreants rummage in lawyers' silky drawers at will*, despite warnings.

For example, the article reports that at least 80% of the largest law firms in the USA have been involved in breaches since 2011.

That's a heads-up for both companies and law firms. Companies with great security might see their confidential information walking out via another back door: their law firm. Similar issues arise too as to other external advisers such as accountants and consulting firms.

In the UK, the equivalent of our Privacy Commissioner – the Information Commissioner – warned lawyers to be careful around data security.[1] Plus the English Law Society issued cloud computing guidelines for solicitors.[2] Those guidelines have been picked up by our own Law Society in *Practice Briefing: Cloud Computing Guidelines for Lawyers*.

1 https://ico.org.uk/.
2 https://www.lawsociety.org.nz/practice-resources/practice-briefings/Cloud-Computing-2014-07-21-v2.pdf.

The Register, in the article above, noted that 173 UK law firms were investigated last year by the Information Commissioners (although we expect quite a few will not be IT breaches, eg, they would include paper based breaches). Raised are issues such as encryption, use of Dropbox, cloud computing, etc.

Law Firms often have Weak 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.[3]

What the Big Corporates are Doing about this Risk with their Law Firms

Large organisations are increasingly recognising this problem and some require stronger defences by law firms. For example, Bloomberg has reported:[4]

> 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.

Teamwork

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.

[3] http://www.americanlawyer.com/id=1202753706763/Cravath-Admits-Breach-as-Law-Firm-Hacks-Go-Public-?slreturn=20160507232301.

[4] http://www.bloomberg.com/news/articles/2015-03-19/cyber-attacks-force-law-firms-to-improve-data-security.

What Cybersecurity Failure led to the Mossack Fonseca Breach?

How Mossack Fonseca was hacked is not known for sure 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.

Continuing the focus on inter-disciplinary expertise and teamwork, which we think is so important in this area, we 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.

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.

Lawyers 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 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.

Legal Standard of Care Required of Law Firms as to Cybersecurity

We turn now to the legal exposure of law firms, noting first that:

- it's really a good case study too for when we advise our clients on cybersecurity issues, as they have many of the same legal issues;
- As Hamish Kynaston explains in his paper, the legal risk is only a part of the risk to be managed by law firms (and by our clients). For example, reputational risk is huge. Imagine if and when it gets out that your law firm has been hacked due to poor security, even if there is no monetary or information loss? That's why we deal with having a crisis management plan below.

A good place to start, when thinking about cybersecurity risk, is IPP5 in the Privacy Act. That is a useful starting proxy for liability more generally, as we explain below:

Principle 5

Storage and security of personal information

An agency that holds personal information shall ensure—

(a) that the information is protected, by such security safeguards as it is reasonable in the circumstances to take, against—

(i) loss; and

(ii) access, use, modification, or disclosure, except with the authority of the agency that holds the information; and

(iii) other misuse; and

(b) that if it is necessary for the information to be given to a person in connection with the provision of a service to the agency, everything reasonably within the power of the agency is done to prevent unauthorised use or unauthorised disclosure of the information.

IPP5 highlights three points:

1. The level of cybersecurity is what is reasonable in the circumstances (the more sensitive the information, the more care is needed).
2. Another key liability area is tort (eg negligence) and that also entails a reasonableness standard. We have illustrated the analysis of the tort of negligence causes of action in the Appendix below, *What Foot and Mouth can teach us about Cybersecurity*. Ditto duties of directors given Companies Act duties on them based on an objective reasonableness standard.
3. When, as often happens, the information is given to third parties, the agency cannot do a Pontius Pilate: it still has duties based on a reasonableness standard as in IPP 5(b). IPP 5(b) also helps sharpen the focus on the key risk arising out of cyber breach via suppliers' systems.

There are other causes of action too, beyond privacy (both in tort (including privacy tort actions where the law is evolving) and under the Privacy Act) and negligence causes of action. For example, there are duties of confidentiality, and duties arising out of industry specific regulation such as the Financial Markets Conduct Act.

And here's a trap as to the firm's contracts: A company may promise its customers that "We will keep your information secure" which is a legally enforceable 100% contractual commitment, quite different from "We will take reasonable steps to keep your information secure." That is not to say the commitment is not made, but it better be made, knowing the risk given 100% security is not possible. For example, should you promise clients 100% protection of their money in your trust account, so you pay them out whether or not you have been negligent?

Then there's off-shore legal risk too.

Those caveats on that reasonableness point shows that legal analysis calls for much more focus than just checking if there is a "reasonable" approach to security.

What is Required for a "Reasonable" Standard?

Reasonableness does not require perfection and cybersecurity steps should reflect the risk as to the particular system and information. Best industry practice will be highly relevant in determining the standard of care that is required, as are industry standards, guidance and so on. Just like assessing a reasonable standard of care for professionals.

That's one reason why there needs to be coordination between, at least, cybersecurity specialists and lawyers.

Our Clients have Legal Responsibility too as to their Information Held by their Law Firms

Our clients also have legal responsibility (and reputational responsibility) for taking steps to ensure we protect their information. This is a good example of duties as to third parties' cybersecurity under for example IPP5 (b).

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.

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, for example.

Teamwork and thinking like a pirate, not a Navy captain

Cybersecurity is not something for lawyers to do in a silo, just as CIOs shouldn't do so. This is a multi- disciplinary area for CEO, ICT, Legal, HR, finance and so on, plus the board too.

Additionally, cybersecurity is not something that fits neatly solely in risk registers and matrices. Says very experienced cybersecurity specialist, Michael Wallmansberger, Chief Information Security Officer at Wynyard Group:

> Working in security requires a certain mind-set (thinking like an attacker; non-linear thinking); the ability to apply a set of well-known (but not always well understood) security principles and patterns; a comprehensive understanding of the underlying technology that makes up the secure systems; and an ability to work across the business on multi-faceted issues including with the CEO and the CFO.

There's a useful Harvard Business Review article that makes similar points, entitled, *See Your Company through the Eyes of a Hacker*.[5] 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

[5] https://hbr.org/2015/03/see-your-company-through-the-eyes-of-a-hacker.

> 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. 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.

Planning for a Cyber Breach

When the IT manager or a reporter phones the managing partner to say there's been a cyber breach, that's not a great time to learn how breaches work and what to do about them. Nor is it a good time for the company's internal people, and external advisers such as comms, legal and technical, to upskill in this area. They must hit the ground running, as a team.

This is not just a commercial and reputational issue: it is a legal duty issue too.

Good plan. Good people. Reduce legal exposure.

For example, as the Australian equivalent of the Privacy Commissioner pointed out in October:

> All entities should have a data breach response plan. Your actions in the first 24 hours after discovering a data breach are often crucial to the success of your response. A quick response can substantially decrease the impact on the affected individuals.

Talk to experts in the field and they'll say the same thing. Michael Wallmansberger notes:

> Cyber incidents are analogous to fire. A well-drilled evacuation plan should prevent loss of life and serious injury if fire breaks out in a modern building. However, unless adequate fire suppression systems are in place and fire trucks are ready to respond, fire may still cause significant economic damage. In cyber security, a good plan will minimise the worst impacts, for example the damage to reputation that comes with appearing uncoordinated and ill prepared. However, a response plan cannot entirely compensate for inadequate protective security controls or limited response capability.

Says Anna Kominik, a specialist in crisis comms, (who presents the IOD's course on Leading through a Media Crisis):

> Be clear on roles and responsibilities, to connect the internal/business continuity with the external/ reputation management in a pressured and time poor environment, where companies and boards are often working with partial information. The plan needs to be kept up to date (for example, cyber security issues change frequently) and road tested. Four out of five business leaders expect their companies will experience a media crisis in the next year, but barely half have a plan to deal with it. A crisis can put board members in front of the media and the public in a way they never anticipated. The best

> advice to boards is ‘have a plan’, not just for cyber breaches, and make sure they’ve practiced it.

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?

Appendix: What foot and mouth can teach us about cybersecurity

Overview

The threat of a digital computer virus is a world apart from the ravages of Foot and Mouth disease. Or is it?

In a 1966 negligence case, the Foot and Mouth virus escaped from a UK research institute and infected neighbouring cattle. The institute was found to owe a duty of care to the affected farmers.

We think the same principle would apply to modern companies that allow digital viruses to escape and infect "neighbouring" users. The law of negligence often proceeds by analogy and here's a last century analogy for a modern time digital issue.

Below, we outline how negligence principles work in practice, and why it's so important to ensure that cyber security measures are up to industry standards from a legal perspective.

The detail

The year is 1959. The Foot and Mouth Disease Research Institute of Surrey, England, has just imported a new virus from Africa for experimental purposes.

The virus escapes, cattle neighbouring the Institute become infected, and the Minister of Agriculture is forced to temporarily close the Guildford and Farnham markets to quarantine the disease.

The market closures (which lasted for 6 days in all) did not please the local auctioneers, Weller & Co, who were unable to carry out cattle auctions during this period. Weller & Co decided to claim for financial losses by suing the Foot and Mouth Institute under the law of negligence.

The court found that, if the virus were to escape from the Institute, it was a foreseeable fact that neighbouring cattle could die.[6] The Foot and Mouth Institute consequently had a legal duty towards the owners of neighbouring cattle to take reasonable care to prevent the disease from spreading.

In the case of Weller & Co, however, their relationship with the Institute was too remote to create such a duty. The auctioneers' claim for financial loss was dismissed.

Why is Foot and Mouth relevant to cyber security?

Imagine a more modern situation. The year is 2016. A company with inadequate cyber security has managed to attract a deadly computer virus. The virus spreads, infecting the company's internal network and online systems. A few hours later, the company goes into digital lock-down to prevent the disease from spreading.

6 *Weller v Foot and Mouth Disease Research Institute* [1966] 1 QB 569, QBD.

Unfortunately, the damage is done. The virus has already infected the systems of sub-contractors, personal devices used by employees, business contacts, website users, and thousands of other third parties.

To whom does our fictitious company owe a duty of care under the law of negligence?

If such a case were to unfold, the court's approach would likely involve applying the same sort of legal principles relied upon last century, well before cyber threats even existed.

Under the law of negligence, a duty of care is owed to another party where there is "a sufficient relationship of proximity" that an act of carelessness by the defendant will likely cause them harm.[7]

The rule is problematic in the context of viruses and other electronic threats. It is quite reasonable to hold that there is "a sufficient relationship of proximity" between any two entities who exchange digital information, or in the case of an internet website, to extend a duty of care to everyone who visits the site. For a large company, this could result in thousands, or even millions, of potential claimants.

Equally, the courts are cautious about imposing a degree of liability which is so wide as to be indeterminate. There may be policy considerations which justify limiting the scope of a duty of care, such as the extent to which victims could reasonably have protected themselves, or that the defendant is only liable if it had (or should have had) specific knowledge about the harm other parties would suffer.[8]

Note that a claim for pure financial loss is certainly possible under the law of negligence (and is the most likely harm caused by a computer virus).[9] The reason Weller & Co did not succeed against the Foot and Mouth Institute was because their relationship was too distant to create a duty of care, not because the type of claim was invalid. Will the same rule apply to a computer spreading a virus to third parties beyond direct contacts?

To be clear, this 50-year-old case is not the full answer on cyber security negligence liability, for the law of negligence has evolved since then. A full answer to a particular scenario involves more detailed review of up to date cases, etc. But it remains a great illustration of how the law works in this area.

What standard of care must a company exercise to avoid negligence liability?

Where a duty of care is found to exist, we move to the second consideration: the defendant must also have failed to exercise a reasonable standard of care. The required standard will generally take account of best practice in the relevant industry, and the nature of the particular virus.

It also adjusts to the conduct and expertise of the defendant. For companies which profess to be IT experts, or rely heavily on digital use as part of their business, the standard of care expected of them will be higher.

---

7 *Anns v London Borough of Merton* [1978] AC 728.

8 NZ Law Commission "Electronic Commerce: A guide for the legal and business community" (1998), Chapter 4: the law of torts.

9 *Hedley Byrne & Co Ltd v Heller & Partners Ltd* [1964] AC 465.

What best practice experts and standards on cyber security say should be done will guide what is the required standard of care. That does not require perfection, as no system can be 100% immune from problems.

While courts are willing to consider the difficulty of taking necessary precautions, that is unlikely to be a compelling argument here, as the threat of a computer virus is both widely known and relatively inexpensive to prevent (compared to the risk posed).

Also important is that the obligation to uphold a standard of care is "an obligation which keeps pace with the times. As the danger increases, so must… precautions increase".[10]

Relying on virus protection software is an insufficient precaution if it is not regularly updated.

What this means in practice

Much like the Foot and Mouth Institute in 1959, modern businesses have a legal obligation to protect their "neighbours" from the threat of viruses. In practice, this means taking care to ensure cyber security measures are up to industry standards.

[10] *Lloyds Bank v Railway Executive* [1952] 1 All ER 1248.