CYBERSECURITY MUST BE A PRIORITY FOR FIRMS

FIONA MCLEOD SC, PRESIDENT, LAW COUNCIL OF AUSTRALIA

At the end of last year the Law Council of Australia launched *Cyber Precedent,* an information campaign developed with cybersecurity experts and government, to help the legal profession defend itself against ever growing cyber threats.

As cybercrime and cyberespionage climbs exponentially across the globe, the campaign will help equip legal professionals with the resources needed to remain on the front foot.

The information resources now available through Cyber Precedent include a list of the essential cybersecurity precautions law firms should take, advice on how to protect against ransomware, a response checklist in the case of a cyber attack, and a cybersecurity toolkit for the education of staff.

Of course, the legal profession is not alone in having to step up its response to this global scourge.

Cybercrime and cyberespionage are among the most serious challenges facing the world today, with significant implications for every sector of the modern global economy.

More than 500 million entities globally are compromised through cyberattacks each year, while hacking tools, and hackers for hire, are proliferating.

Individuals, organisations, and nation states are looking to breach computer networks to commit any number of crimes — from sabotage, through data theft, to insider trading, and far beyond.

Despite this, it is fair to say cybersecurity remains an issue we have not normalised as part of our everyday lives and operations — in business, in politics, and within the legal profession.

The threat is becoming harder and harder to ignore, however.

In the United States, for example, a particularly high profile hack hit the networks of Cravath Swaine & Moore LLP and Weil Gotshal & Manges LLP recently.

The assumption is they were looking to steal confidential information for insider trading, or potentially blackmail.

The full investigation, however, will drag on for years, because it is such a complex matter to piece together exactly what was accessed.

Often the case with these kind of attacks is that the first indication of what has been stolen comes when the information gleaned is used maliciously.

The Cravath/Weil attack should be acutely disturbing for legal professionals, because the motives appear to be so clear.

The possibilities for malicious behaviour, if the private information of law firms is accessed by people who know what they are doing, are near limitless.

Just consider the kind of highly sensitive information the legal profession has that could be viewed as a glittering prize for cybercriminals.

There is sensitive client and firm business information, confidential client business information, and client intellectual property.

Corporate clients, in particular, will often have shared details about undisclosed mergers and acquisitions that could be stolen and used easily for insider trading.

There are also litigation and negotiation strategies, settlement parameters, and analysis of evidence that can be used by an opponent.

All this is patently alarming. Yet it becomes even more so when you consider how these threats fundamentally strike at the core of what it is that we do as legal professionals.

Client confidentiality is the very bedrock of the client/lawyer relationship. The importance of trust in this area can scarcely be overstated.

As the Australian Bureau of Statistic's "#censusfail" of 2016 demonstrated, even well-established trust is a flimsy thing. It can be critically damaged in an instant by cybercriminals.

So not only are law firms, and lawyers more broadly, an attractive target for sophisticated hackers — we are also highly sensitive to such attacks

It is fundamental, therefore, that lawyers are able to demonstrate to their clients and regulators that they understand the nature of risk and are adequately prepared to address the threat.

The number of ways through which law firms may be threatened by cybercrime or cyberespionage is also a major concern.

Sometimes attacks — like the attacks on Cravat Swaine & Moore and Weil Gotshal & Manges — are obvious and spectacular.

Yet there are so many other ways law firms are vulnerable.

Ransomware – computer malware that installs covertly on a victim's computer, executes a cryptovirology attack that adversely affects that computer, and then demands a ransom payment to restore it – is rife.

It infects systems and devices via phishing emails and texts, as well as compromised websites, and "malvertising."

Ransomware is not actually new — the first known case was in the 1980s. But its prevalence, and the sophistication of its business models, is on a very steep rise.

A 2015 survey from the Australian Cyber Security Centre in Australia found that ransomware was the most prevalent type of incident affecting Australian businesses, with some 72 per cent of respondents affected.

The conservative estimate is that at least $5 million annually is extorted via ransomware from victims.

The real figure could in fact be much higher, given that many firms will simply choose to pay the ransom, given that the amount demanded is, on average, only $200.

HOW CAN LAW FIRMS AVOID BEING HELD RANSOM?

As is the case in so many areas, it is often the seemingly simple and obvious actions that are too often overlooked.

Although it is the elaborate "heists" that tend to make the headlines, data breaches are more typically caused by simple human error, or by poor internal controls, or through deficient system infrastructure.

Managing this incredible range of risk must become a core priority for law firms.

Some simple preventative measures include:

- Implementing a strong password policy requiring all users to regularly change passwords and requiring more complex passwords, i.e. mixture of lower and uppercase letters, numbers, and symbols
- Making sure all network patches and anti-virus software are updated regularly
- Reviewing and auditing all permissions in your network
- Updating and deactivating all user accounts regularly
- Deactivating and off-boarding departing employees
- Walling off, or segregating users and certain sensitive data
- Changing network and Wi-Fi passwords regularly

While such measures may sound prosaic, it is fair to say there is still a level of complacency within the legal profession that is not at all commensurate with the seriousness of the threat faced.

Some recent research from the legal sector in the UK, for example, indicates 70% of firms do not place cyber resilience within their top five risks, while 85% of firms do not have a documented strategy to improve cyber resilience.

MAKING CYBERSECURITY A TOP PRIORITY

Yet the central point is not adhering to a set checklist, but rather recognising that cyber risks should evolve beyond being seen as an "IT issue".

Mitigating the risks has to be managed by a strategic and coordinated approach, and that means making cyber security a strategic objective.

At senior management level — and even at board level — there must be an acute sensitivity to cybersecurity threats to foster a culture of vigilance.

Yet ultimately if the legal profession's cyber defences are to evolve effectively to keep pace with the changing techniques of foreign adversaries firms need to start acting more holistically and cooperatively, both with each other and with government agencies.

Currently, Australian firms and practices tend to manage cyber risks individually, but this means a fairly common threat is being handled in a diverse and disparate range of ways.

It is inefficient and creates something of a 'broken line of defence' to innovative cyber criminals.

Yet there are now promising green shoots in the coordination space.

The federal government recently launched a national cyber security strategy to help businesses and organisations protect their interests online. Although still in its early phases, this Cyber Security Strategy will likely include the development of mechanisms such as alert systems, to advise law firms and chambers they may be specifically targeted by foreign adversaries.

The Law Council will also continue to develop and advance *Cyber Precedent,* working in partnership with the legal profession, our Constituent Bodies, industry, and government.

As a profession we are in the early stages of formulating an appropriate defensive approach, and the mitigation strategy will need to continually evolve.

The vital point is that the success of our approach will largely depend on our capacity to cooperate, both across the profession and with government. B