Law Council OF AUSTRALIA
Legal Practice Section
Australasian Law Management Journal

Edition: April 2021

Cyber extortion – a guide to your legal and ethical considerations

At a time when ransomware attacks are becoming more common and aggressive, law firms need to educate their employees about cyber risks and understand their professional obligations if they become a victim of hackers, writes Simone Herbert-Lowe.

What is ransomware?

Ransomware is a type of malicious software (malware) that infects computers and makes data unreadable unless a ransom is paid. The ransom demanded will usually be in cryptocurrency such as Bitcoin. Where reliable backups of data are available, it may be possible to recreate businesses' records without paying a ransom. However, this is not always possible, particularly if backups have also been encrypted.

In terms of cybercrime, ransomware is reported to be the fastest-growing type. Recent months have seen a spate of media reports about ransomware attacks on businesses around the world. In Australia, organisations which have been targeted Nine Entertainment, Eastern Health, Law in Order and Toll. Some ransomware threatens not only to encrypt data, but also to publish or sell it. This threat can have serious implications for organisations including law firms with special duties to maintain confidentiality of information.

What high-profile cases have involved law firms?

In May 2020, US law firm Grubman Shire Meiselas & Sacks, which acts for numerous celebrity clients, confirmed it had been the victim of a cyberattack in which hackers accessed 756 gigabytes of data contained in legal files held on behalf of dozens of clients. When it became clear the ransom of US$42 million would not be paid, the hackers reportedly started auctioning off files to the highest bidder.

Law Council OF AUSTRALIA Legal Practice Section
AUSTRALASIAN Law Management Journal

The threat to publish information is clearly a nightmare scenario for a legal practice that holds information it is required to keep confidential. While this US case is an extreme example, Australian law firms have also been victims of ransomware. Lawyers are, of course, expected to uphold the law, so what factors should be considered in the event of a ransomware attack?

What are the public policy considerations?

There are strong public policy reasons why ransoms should not be paid – namely to discourage further escalation in this type of crime, and the Australian Cyber Security Centre and law enforcement bodies recommend against making ransom payments. There is no guarantee that cybercriminals can or will decrypt your records if a ransom is paid and paying a ransom could also make you a target for further attacks. In September 2020, the former head of the UK's National Cyber Security Centre reportedly called for the UK government to make it illegal for companies to pay cyber hackers a ransom, describing ransomware as "the single biggest contemporary scourge in cyber space".

Is it legal to pay a ransom?

While it is generally accepted that in Australia payment of a cyber ransom is not illegal, it is a serious offence to contravene anti-money-laundering legislation (*Criminal Code Act 1995* (Cth), division 400) or to make funds available to an organisation where a person knows or is reckless as to whether the organisation is a terrorist organisation (*Criminal Code Act 1995* (Cth, s 102.7), or to an organisation proscribed by UN sanction (*Charter of the United Nations Act 1945 (Cth)*).

Some commentators have suggested a defence of duress might be available in certain circumstances – and where there is any possibility these issues could arise, you should seek specialist advice. Organisations subject to anti-money-laundering legislation may also be required to disclose the payment of a ransom.

What do the professional rules of conduct state?

The *Legal Profession Uniform Law Australian Solicitors' Conduct Rules* (rule 3) provide that a lawyer's paramount duty is to the Court and the administration of justice. However, where there is no clear contravention of that duty the obligation to protect the clients' interests is

otherwise paramount (see D. Bowles, "Is it ethical (or legal) for law firms to pay cyber-ransom?", Queensland Law Society, December 2017).

Where a lawyer receives what appears to be a credible threat to publish confidential information held on behalf of others, he or she will need to consider how professional obligations might apply. Under the Australian Solicitors Conduct Rules, which now apply to most Australian lawyers:

- Rule 4.1.1 provides there is a duty to act in the client's best interests; and
- Rule 7 requires clear and timely advice to assist clients to understand legal issues and make informed choices.

Other factors to consider are the fiduciary relationship between solicitor and client, based on the relationship of trust that the client has placed in their lawyer, and the equitable duty to maintain the confidentiality of communications. There may also be duties to maintain the confidentiality of information pertaining to third parties and, if your firm is subject to the *Privacy Act 1988*, a duty to report an eligible data breach involving personal information where the data breach is likely to result in serious harm to any of the individuals to whom the information relates.

What preventative action can firms take?

The choice between paying a ransom and either losing all your business records or seeing confidential client information lost or published is one that no legal practitioner ever wants to make.

Minimise your risk by making regular backups that aren't connected to your network, use antivirus software, and keep operating systems and software up to date. Given that most ransomware is delivered via a phishing email, ensure everyone in your practice is educated about cybercrime and knows how to recognise suspicious emails.

Lastly, if you have cyber insurance you should notify your cyber insurer immediately and obtain its consent before making any payment.

Law Council OF AUSTRALIA
Legal Practice Section
AUSTRALASIAN Law Management Journal

The key takeaway messages:

- While payment of a cyber ransom is a last resort in Australia, it is generally not illegal.
- However, possible offences under anti-terrorism and anti-money laundering legislation should be considered.
- Ethical issues for lawyers to consider include duties to the administration of justice, to act in the client's best interests and to maintain confidentiality.

Simone Herbert-Lowe is the Legal Practitioner Director of Law & Cyber, a provider of cyber education and legal advice for businesses affected by cyber events. Simone is the author and presenter of the online course, Cyber Risk for Law Firms.