Is it Ethical (or legal) for law firms to pay cyber-ransom?

To pay or not to pay? That is the question. What are the ethical, legal and practical constraints on a law firm paying cyber criminals to recover data lost to a cyber-intrusion?

One of the most reliable ways of monetising cybercrime is demanding ransom payments to decrypt locked networks or prevent disclosure of secrets. The amounts demanded are often low, at least in comparison to the cost of the potential losses otherwise, although there is no guarantee that the agreement will be honoured[1].

But can a legal practitioner knowingly pay a criminal? By doing so, are we participating in their offence? Is the objection a question of ethics or something else? There are arguments in both directions:

The "don't pay" case: Cyber-crime is the fastest growing crime in the world, doubling in number and impact year on year.[2] The Hacktivist and mischievous individuals of the past are being replaced by IT professionals working in 9 - 5 businesses that happen to make their profits from cybercrime, or by providing outsourced hacking services to criminal networks, terrorists and cash-strapped governments. The reason for this growth curve is simple - low risk and high profit.

Making such payments creates a revenue stream for criminals. Every dollar in profit will increase both the capacity and incentive for tomorrow's attacks and there is a consequent public policy objection to paying ransoms generally.[3] Australians' inclination to roll over and pay potentially increases our attraction as a target compared to others in Asia.[4] A Legal Practitioner's duty to the Administration of Justice,[5] and general obligation of honesty[6] renders it inappropriate for us to participate in, encourage or facilitate unlawful conduct,[7] even if such participation is not unlawful in itself.[8]

The case for payment: the victim of any crime is not the author of his or her own misfortune. A ransom payer is no more responsible for the underlying crime than a person robbed at knife point. A lawyer is no more obliged to suffer avoidable consequences of a cyber attack than they are obliged to risk being stabbed to prevent a drug addict stealing their wallet.

In most cases it is client data and client interests that will be affected. A Solicitor's duty of loyalty to a client requires us to take all lawful steps to protect such interests, subject to our broader duties to uphold the administration of justice.

In *Masefield AG v Amlin Corporate Member Ltd*[9] Rix, LJ considered the payment of a ransom in the context of a ship seized by pirates:

> *"there is no universal morality against the payment of ransom, the act not of the aggressor but of the victim of piratical threats, performed in order to save property and the liberty or life of hostages … there is no universally recognised principle of morality, no clearly identified public policy, no substantially incontestable public interest, which could lead the courts, as matters stand at present, to state that the payment of ransom should be regarded as a matter which stands beyond the pale, without any legitimate recognition. There are only elements of conflicting public interests, which push and pull in different directions, and have yet to be resolved in any legal enactments or international consensus as to a solution …"*

---

[1] According to surveys reported from the UK, 1:3 attackers pocket the ransom without successfully unlocking the data: http://www.theregister.co.uk/2016/09/07/uk_ransomware_victim_survey/.

[2] Australian Cybercrime Online Reporting Network (ACORN) cumulative statistical reports: https://www.acorn.gov.au/resources.

[3] Proceedings, Senate Standing Committee on Foreign Affairs, Defence and Trade: Australian Government's response to kidnapping of Australians overseas 2011, findings Chapter 4, para 4.10.

[4] https://www.telstra.com.au/content/dam/tcom/business-enterprise/campaigns/pdf/cyber-security-whitepaper.pdf.

[5] *Australian Solicitors Conduct Rules 2012* ('ASCR'), rule 3.

[6] ASCR, rule 4.1.2 and rule 5.1.

[7] *Leary v Commissioner of Taxation [(Cth.)* (1980) 47 FLR 414 at p 435; *D'Orta-Ekenaike v Victoria Legal Aid* [2005] HCA 12.

[8] *In Re B* [1981] 2 NSWLR 372 per Moffitt, P at 381-2.

[9] [2011] EWCA Civ 24.

As an aside, if the attackers have had access to compromised systems there is a clear ethical duty to warn clients that this has occurred. So "pay up and keep quiet" is only possible where there is no way the intruders could have client data.

As another aside, before you pay, check whether there is a free unlock tool available on the net: https://www.nomoreransom.org/en/index.html. Prior to making a payment or electing to remedy the problem in another way, it is suggested that the firm seek the views of their insurer.

Decision time: On balance, the clear obligation to protect client interests tends to outweigh the general public policy objection to paying criminals. Payment of the ransom is therefore an option available to the firm once all of the competing alternatives have been considered.

The duty to uphold the administration of justice is undoubtedly a solicitor's first duty, but there must be a reasonably clear contravention of that duty to invoke paramountcy over a client's interests. If lawful, we are entitled to make the decision based on what we think will lead to the best outcome for the client and our firm. But one word of caution – the payment may, in some circumstances be unlawful.

The legality of ransom payments by Australians: Prima facie it is unlawful[10] to pay a ransom to a terrorist organisation[11] or an organisation proscribed by UN sanction.[12]

An offence is committed when a person makes funds available to a "terrorist organisation", knowing or reckless to the fact that it is such. "Reckless" is defined quite widely, but still requires some degree of knowledge that the perpetrator is likely to be a proscribed group. While in most attack scenarios the identity of the perpetrators is not known, there are recent examples where a political motive is stated, the Feb 2017 attack on the National Health system in the UK, for example.

As in all ransom payment scenarios, a defence of duress may be available. To establish the defence the payer must show that (1) there is no reasonable way that the threat can be rendered ineffective and (2) the conduct is a reasonable response to the threat.[13]

In the case of a pure crypto lock attack (ie, where there is no way the confidential information can be published), presuming the data can be restored from back up, it is hard to see that limb (1) of the defence could be made out. Even if the reinstatement of the data is onerous and expensive, it is likely that it is the required option.

Even where there is no other way to prevent release, a person wishing to avoid the release of information that will damage their business is obviously in a very different position to a person seeking to preserve the life of a kidnapped family member. The "reasonable response" requirement may also be difficult to establish. There is no mechanism for seeking prospective approval for such a payment in advance of it being made.

Where there is any reason to believe that an embargoed or prohibited organisation will be the recipient of the payment, a practitioner should seek specialist legal advice prior to making it.

David Bowles
Ethics Solicitor
8 December 2017

[10] *Criminal Code Act* 1995 (Cwth) s 102.1(a), 102.7, 103.2(1); *Charter of the United Nations Act* 1945 which provides the domestic legislative backing to the UN sanctions framework, most pertinently the *International Convention for the Suppression of the Financing of Terrorism* on 9 December 1999 (resolution 54/109).
[11] *Criminal Code Regulations* (2002) Cwth.
[12] Australian Government, Department of Foreign Affairs and Trade: UN Sanctions prohibited organisations list.
[13] *Criminal Code Act 1995* (Cwth), s 10.2.