When held to ransom: Legal implications of ransomware attacks for legal practitioners and their clients

BROOKE HALL-CARNEY, AMY COOPER-BOAST AND ELIZABETH CARROLL-SHAW, LK LAW

As ransomware attacks accelerate in scale, frequency and sophistication, they pose a risk both to legal practitioners and their clients. It is not only government, critical infrastructure and large corporates falling victim: over 60% of Australia's small to medium businesses have now experienced a cybersecurity incident.[1] The professional services sector is emerging as a ransomware target[2] – perceived as data-rich and motivated to protect client confidentiality or privilege. In a quickly evolving regulatory and threat landscape, it is critical for practitioners to understand the legal implications of ransomware incidents for their practices and for their clients.

THE NATURE OF THE THREAT

Ransomware involves the use of malicious software to infiltrate and lock data or systems and demand payment for their release. Simpler models of attack involve cybercriminals encrypting files and demanding payment (typically in cryptocurrency) for a decryption key.

The past year saw a rise in 'double' and 'triple' extortions.[3] With ransomware victims choosing to restore data from back-ups rather than pay a ransom, or being unable to pay where uninsured or under-insured, cybercriminals have pivoted to exfiltration (covert extraction) of data. After exfiltration, two ransom demands follow – the first in exchange for unlocking the system or data; the second in exchange for not selling the data on the dark web, or releasing it publicly. A third ransom demand may be made directly to the victim's clients or suppliers, whose confidential information was compromised – or, alternatively, the threat of compromising clients or suppliers is used as leverage against the victim.

A market for Ransomware-as-a-Service (RaaS) has emerged, with developers offering malware as a product for sale to hackers for a fee or a commission paid from the ransom.

PAYING CYBERCRIMINALS

The Australian Cyber Security Centre (ACSC) is the Federal Government's lead agency for cybersecurity. The ACSC's position on ransomware payments is clear: payments are never condoned, do not guarantee a return of stolen data or system access, and perpetuate a vicious circle by funding cybercriminals. Some organisations adopt a policy to never pay; for others, where health or safety is put at risk, payment is more readily justified. A 2021 global survey indicates that of those attacked, a quarter paid the ransom, with the average ransom rising by 63% year-on-year.[4] Ransoms are highest in the Asia-Pacific, averaging US$2.35 million.[5]

In practice, a victim's options when faced with a ransomware demand are influenced by complex factors: the severity of the attack; the sensitivity of compromised data; the extent to which data has been exfiltrated; the feasibility, time and cost of either data restoration (from back-ups) or decryption; business continuity; reputational, ethical, financial and insurance considerations; and the risk that paying a ransom will attract future attacks.

Victims must also grapple with the legality of paying a ransom. Ransomware payments are not specifically prohibited under Australian law. A payment could, however, offend anti-money laundering and counter-terrorism financing legislation where a victim holds sufficient knowledge as to the cybercriminal's identity and possible use of the funds.[6] If an illegal payment was made, a defence may arise in circumstances of duress, sudden or extraordinary emergency or self-defence (of persons or property).

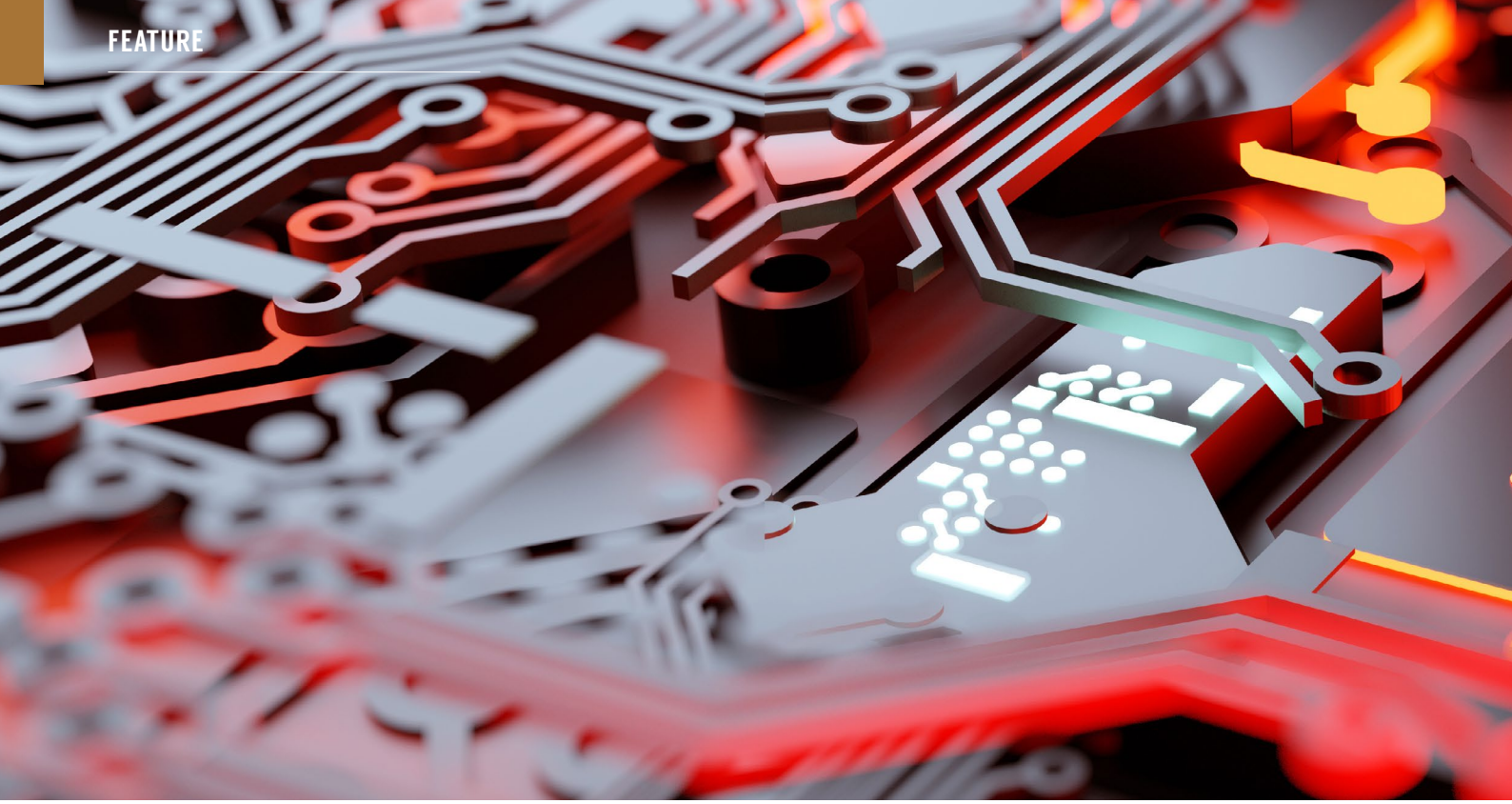
Paying a ransom would also constitute an offence under Australian law if made to persons or entities proscribed by UN or Australian sanctions, or in contravention of sanction laws.[7] A defence arises for bodies corporate who prove they undertook reasonable precautions and due diligence to avoid a contravention.

WHO TO NOTIFY

Ransomware victims will need to consider their communications with affected persons, insurers and stakeholders. They may be required to disclose the incident under third party contracts. A cybercrime police report can be made via the ACSC.

Various notification regimes also operate:

- Organisations with an annual turnover exceeding $3 million (amongst others) must report 'eligible data breaches' and notify affected individuals under the *Privacy Act 1988* (Cth).
- Responsible entities for specified critical infrastructure assets will be required to report cybersecurity incidents.[8]
- Reporting entities under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) have suspicious matter reporting obligations.



- ASX-listed entities should consider their continuous disclosure obligations. Disclosure may also be required in an entity's financial reports.
- Financial institutions must report 'material information security incidents' under APRA Prudential Standard CPS 234.
- Mandatory notification schemes apply in the health, defence, aviation and maritime transport sectors. Organisations may be required to liaise with other sector-specific regulators.
- Australian businesses with international establishments or activities may have reporting obligations under foreign laws and regulations, such as the EU or UK *General Data Protection Regulation*.

RANSOMWARE REFORM

Regardless of the outcome of the Federal election, further ransomware reform is imminent, with both major parties releasing competing ransomware strategies.[9]

Two Opposition bills have proposed mandatory reporting of ransomware *payments*. The Federal Government has foreshadowed mandatory reporting of ransomware *incidents*. At the time of writing, both regimes are proposed to apply to businesses with an annual turnover of $10 million or more.[10]

On 17 February, 2022, the Federal Government introduced the Crimes Legislation Amendment (Ransomware Action Plan) Bill 2022 (Cth). This Bill criminalises ransomware activities, RaaS and cyber-attacks on critical infrastructure, but does not introduce criminal or accessorial liability for making ransomware payments. By contrast, the Opposition has called for regulation of payments through measures such as government pre-approval.[11]

LIABILITY FOR ORGANISATIONS AND DIRECTORS

A high alert issued by the ACSC in February, 2022 requested all Australian organisations to '*urgently*' adopt an enhanced cybersecurity posture, as geopolitical tensions rose with the attack on Ukraine.[12] Businesses may be exposed to ransomware attacks through their own security lapses or through supply chain vulnerabilities.

In addition to theft or destruction of data and physical assets, reputational damage and financial losses, a ransomware attack can expose a business to litigation risk. Claims may be brought by clients or suppliers whose sensitive data has been stolen or leaked, or by contractors impacted by business disruptions.

It is incumbent on organisations to consider mitigation measures such as:

- Enhanced cybersecurity controls.[13]
- Staff education and simulations.
- Contractual protections, such as cybersecurity requirements for suppliers and tailored force majeure clauses.
- Multi-disciplinary response and continuity plans.
- Cyber insurance (noting that it can be difficult to acquire, expensive and subject to exclusions and may cede control to an insurer).
- Secure and regular back-ups and offline or 'cold' storage – key tools in avoiding many ransomware payments. Back-ups will not, however, solve the dilemma of particularly sensitive data under threat of public release; albeit neither will be paying the ransom, with any degree of certainty.

Although it has discussed mandatory or voluntary cybersecurity governance standards for large businesses,[14] the Federal Government has not, to date, enacted any personal director liability for inadequate cyber protections. However, a director's duty to act with care, skill and diligence will be breached by failing to prevent conduct carrying a foreseeable risk of harm to the interests of the company.[15] Having regard to the deteriorating cyber threat environment, it is increasingly likely that courts will consider inadequate cybersecurity measures to pose a foreseeable risk of harm. ASIC has also recently emphasised the active role it expects from directors in managing cyber risk.[16]

Last year, ASIC commenced its first action against an entity for cybersecurity shortfalls. The entity, which is alleged to have breached financial services licensee obligations, experienced ransomware and other attacks.[17]

PITFALLS FOR LEGAL PRACTITIONERS

Perhaps unsurprisingly, the legal profession is an attractive target for ransomware due to the valuable and sensitive nature of information held on behalf of clients. Most ransomware attacks in Australia are reported in the legal, accounting and management services

sector.[18] Ransomware attacks may target legal practices directly, or may seek to exploit interdependencies with professional networks and service providers.

As well as notification obligations and exposure to loss and liability, legal practitioners must consider their professional responsibilities. A failure to implement appropriate protections may result in breaches of fiduciary, tortious and contractual duties to clients; a breach of the *South Australian Legal Practitioners' Conduct Rules* requiring maintenance of client confidence and competent, diligent delivery of legal services; and claims of unsatisfactory professional conduct or professional misconduct. Any ransomware payment would also require careful ethical navigation.

Case examples highlight pitfalls of ransomware and other cyber-attacks for lawyers and their clients:

- Law practices should ensure that important information, such as client data, retainer agreements and costs disclosures, is protected and backed-up.[19]
- Ransomware attacks can compromise data relevant to proceedings, causing evidentiary and discovery issues.[20] This can lead to loss of evidence, and cost and difficulties in restoring files (if restoration is possible). Where litigation is anticipated or on foot, it is vital to ensure that relevant documents are securely backed-up.
- A UK firm's failure to implement multi-factor authentication, patches and encryption, whose sensitive court bundles were released on the dark web by ransomware criminals, led to a £98,000 regulatory penalty.[21]
- Legal professional privilege is not an actionable legal right. It cannot found an application to claw back or prevent the use of privileged documents where they are stolen from a law firm's computer system and publicly disseminated.[22]
- The impact of a cyber-attack can be far-reaching, as illustrated by the law firm subject to the Panama Papers data spill. The infiltration of Mossack Fonseca's systems and release of confidential documents led to severe reputational and financial consequences for the firm, and its closure two years later. **B**

Endnotes

1 *This article is current as at 11 March 2022.* Cyber Security Industry Advisory Committee, *Locked Out: Tackling Australia's ransomware threat* (March 2021) p.2.
2 Australian Cyber Security Centre, *Annual Cyber Threat Report 2020 – 2021* (15 September 2021), p.21, Figure 8.
3 Australian Cyber Security Centre, *2021 Trends Show Increased Globalized Threat of Ransomware* (10 February 2022).
4 Crowdstrike, *2021 Global Security Attitude Survey*, p.10.
5 Ibid.
6 *Criminal Code Act 1995* (Cth), *Criminal Code* Part 5.3, Division 103 and Part 10.2, Division 400.
7 *Charter of the United Nations Act 1945* (Cth) ss. 21 and 27 and *Autonomous Sanctions Act 2011* (Cth) s.16.
8 Under Part 2B of the *Security of Critical Infrastructure Act 2018* (Cth), once the rules 'switching on' these obligations are registered and a three-month grace period has passed.
9 Department of Home Affairs, *Ransomware Action Plan* (October 2021); Federal Labor, *Beyond the Blame Game: Time for a National Ransomware Strategy* (February 2021).
10 See the Opposition's Ransomware Payments Bill 2021 (Cth) and Ransomware Payments Bill (No 2) 2021 (Cth) and Department of Home Affairs' medial release, *New plan to protect Australians against ransomware* (13 October 2021). The Opposition's proposal would additionally apply to Government entities.
11 Federal Labor, *Beyond the Blame Game: Time for a National Ransomware Strategy* (February 2021), pp.14 – 16.
12 Australian Cyber Security Centre, *Australian organisations should urgently adopt an enhanced cyber security posture* (23 February 2022; updated 4 March 2022).
13 This ought to include, as a baseline, the ACSC's 'Essential Eight' strategies: see <https://www.cyber.gov.au/acsc/view-all-content/essential-eight>.
14 Department of Home Affairs, *Strengthening Australia's cyber security regulations and incentives: An initiative of Australia's Cyber Security Strategy 2020* (July 2021); industry consultation closed in August 2021.
15 *ASIC v Cassimatis* (2016) 336 ALR 209.
16 ASIC Chair Joseph Longo, '*ASIC's corporate governance priorities and the year ahead*' (Speech delivered at the AICD Australian Governance Summit, Melbourne Convention Centre, 3 March 2022).
17 *ASIC v RI Advice Group Pty Ltd* [2021] FCA 1193.
18 Office of the Australian Information Commissioner, *Notifiable Data Breaches Report: July to December 2021* (22 February 2022), pp. 23 – 26.
19 *Leung v Fordyce (t/a Pmf Legal Trading)* [2019] NSWSC 18.
20 *In the matter of Beverage Freight Services Pty Ltd* [2020] NSWSC 509; *Cargill Australia Limited v Viterra Malt Pty Ltd (No. 28)* [2022] VSC 13.
21 Information Commissioner's Office (UK), Monetary Penalty Notice issued under *Data Protection Act 2018* to Tuckers Solicitors LLP (28 February 2022).
22 *Glencore International AG v Commissioner of Taxation* (2019) 265 CLR 646.