Cyber security

The new frontier for commercial lawyers

All businesses, whatever the size, need to appreciate the risk posed by cyber crime. The initial damage done by the hacker is exacerbated by secondary liability costs including legal proceedings from vendors, credit card payment processors, consumers and of course, regulators. The clean-up can be catastrophic.

Technology has revolutionised the commercial world. Cloud and the use of BYOD (bring your own device) allow for faster access to corporate networks and can drive profitability with flexible work practices.[1] Businesses are attracted to this new technology, but some are wary because of the unknown risks. Such a risk is cyber crime. An ignorance of cyber crime either makes businesses vulnerable, or makes them risk sceptical of new technology, preventing them from achieving their potential.[2] It is the job of commercial lawyers to ensure that we provide our clients with advice that can support technology evolution while mitigating the risk posed by cyber crime.

Potential risks for businesses

Hacking is a prime risk for any business that stores personal client data or confidential information. Hacking is where an intruder gains unauthorised access to a network to interfere with data stored on a computer. Hackers use specialised tools and target specific sites or networks on the internet.

Large corporations like Mastercard, Paypal, and Sony, all of whom have suffered public cyber attacks, are not the only targets. According to Verizon's 2011 Data Breach Investigations Report, hackers are increasingly setting their sights on small to medium-sized enterprises (SMEs). SMEs present easy targets for organised cyber crime because they often have weaker security. For example, in December 2012, Russian hackers held an Australian medical centre to ransom by encrypting sensitive patient information on the centre's server.[3] The centre's only practical option was to pay. While the ransom was relatively low ($4000), the inability of the centre to access medical records put patient safety at risk.

Impacts of cyber crime on businesses

Cyber crime poses multiple threats to businesses including: online fraud, online hacking, theft of confidential data

ISTOCKPHOTO

and intellectual property (IP), money laundering, "phishing" and ID crime. The impact of such crimes inevitably reverberates beyond the initial crime itself.

Some of the main impacts of cyber crime on businesses include:

- loss of data, innovative intellectual property, confidential or commercial information;
- lost sales (i.e. denial of service [DoS] attacks by shutting down payment services);
- loss of reputation and consequently, market confidence; and
- financial cost associated with cyber attacks including costs of compulsory notification, damages payments and fines.

One of the most notable consequences of cyber crime is the potential liability a business may owe to its clients or customers who, for example, may have experienced a breach of their confidential information, or suffered financial loss from theft or fraud. Hence, it is important that businesses are aware of their responsibility to protect confidential information, especially in jurisdictions like Australia where breaches of privacy can result in fines.

Cyber crime touches a wide range of law, and legal development on cyber crime is expanding.[4] While cyber crime is covered by the criminal law,[5] in practice, the law hardly deters the cyber criminals. In contrast, criminals feel safe because national jurisdictions make law enforcement difficult and the anonymity of the internet obscures criminal identity.

Cyber crime is a double whammy for businesses that find themselves under attack. Not only is there the potential liability for private claims; there is also the possibility of enforcement by regulatory bodies like the Australian Information Commissioner (AIC).

Privacy law

Australian privacy law is a mix of federal and state/territory legislation. Currently, federal law requires that any personal information held by an organisation must be protected by appropriate security measures.[6] The future amendments under the *Privacy Amendment (Enhancing Privacy Protection) Act* 2012 (Cth), coming into force from March 2014, present a tougher privacy regime. Under the new regime, AIC can impose fines of up to $220,000 for an individual and $1.1 million for organisations that seriously, or repeatedly interfere with the privacy of individuals.[7] The organisation may be required to redress any loss or damage suffered by the victim of cyber crime. This is key for businesses that hold personal data, as a careless or unknown breach of their systems could result in regulatory action by way of fines. A breach of privacy law due to cyber crime increases financial risk for companies on two levels: first, there is a potential liability to pay financial compensation to victims and second, there are pecuniary penalties from the regulator.

IP law

Loss of data through hacking is not limited to personal information. Potentially more damaging is the loss of confidential information owned or used by businesses, including IP rights. IP includes creative works protected by copyright, brand identification protected by trademark and creative inventions protected by patents. Theft of this information could result in loss of commercial advantage, breach of licensing/use requirements and breach of contract where the information is owned by a third party. The losses to businesses from IP rights infringement can be significant, including legal costs of defending or settling IP infringement claims. Therefore, businesses that store these kinds of data should ensure strong protections from hacking are in place. Additionally, staff training and awareness about the danger of cyber attacks can help in protecting business data and systems.

Contract law

Ordinarily, internet service providers (ISP) are not held liable for the creation or propagation of worms, viruses and other malware.[8] However, businesses can protect themselves through contract by requiring that their ISP enforces processes and undertakes regular network connection amendments to prevent customers from suffering from a DoS attack.[9] A breach of this condition can provide a mechanism for the business to seek damages from its ISP.

Tort

While the case law is limited in this area, another argument might be made that the tort of trespass as we know it in the physical sense could be applied to the cyber landscape. By not having adequate security measures in place, are you creating an implied right of entry into your networks? The tort of trespass could be invoked if you inadvertently allowed your corrupted network to transfer a worm or virus to your mail recipients by the notion of "negligent transmission".[10]

Finally, cyber security and crime are always hot topics for the media. Reputation protection in a competitive business world needs to focus on keeping client data and material secure. A business that cannot protect itself against cyber attack will not survive in the e-world in which we live. ▮

JACOB SMIT is a law graduate and **KATIE CLAPHAM** is a para legal at DLA Piper in the intellectual property and technology practice. The content of this article is for informative purposes only and does not constitute legal advice.

1 Andrew Walker-Brown, "Managing VPNs in the mobile worker's world" (2013) 1 *Network Security* 18.
2 Note 1 above.
3 Sara Hicks, "Russian Hackers hold Gold Coast doctors to Ransom", *ABC News* (11/12/2012).
4 See e.g. *Foxtel Management Pty Ltd & Anor v MOD Shop Pty Ltd and Others* (2007) 72 IPR 1; *Intelmail Explorenet Pty Ltd and Anor v Vardanian and Anor (No 2)* (2009) 82 IPR 281.
5 *Larkin v The Queen* [2012] WASCA 238.
6 Alec Christie & Reyhaneh Saadati, "Australia" *Data Protection Laws of the World* (DLA Piper, March 2013) 15, 16.
7 Note 6 above.
8 Dough Lichtman and Eric Posner, "Holding Internet Service Providers Accountable", *John M Olin Law and Economics Working Paper No. 217 2nd Series*, (University of Chicago, 2004) 1.
9 Attorney-General's Department, *Managing DoS Attacks* (2006) www.dbcde.gov.au/__data/assets/pdf_file/0011/41312/DoS_Report.pdf .
10 See: Title 18, USC, § 1030(a)(5), H. Marshall Jarrett et al, *Prosecuting Computer Crimes* (Office of Legal Education for United States Attorneys) 36. avail online: www.justice.gov/criminal/cyber crime/documents.html.