Cyber duty of care

How to minimise cyber vulnerability in the practice of law

EJ WISE Wise Law – www.wiselaw.com.au

This article[1] is designed for legal practitioners to quickly identify areas within their firm or legal practice which need regular review in order to ensure compliance with relevant laws, regulations, standards, and guidelines, as well as help you meet basic client expectations/client obligations.

While most practitioners are busy with the myriad elements in running or participating in a modern legal practice, it is easy for fundamental data obligations to remain unchecked. In the most recent quarter from 1 October to 31 December 2018 the legal industry ranked third worst in all of Australia (out of the top five industry sectors that reported privacy breaches). Alarming when we legal practitioners are the trusted advisers and clients act in reliance upon our diligence both in holding personal data/use of technology and their advice regarding the client's own cyber vulnerabilities and risks. The client's rights include the ethical and safe handling of their information.

Technologies and their coincidental obligations have brought legal practices under the spotlight as places of business holding distinctly private, personal, proprietary, strategic and privileged information or data.

Legal clients and society reasonably expect that practitioners are fulfilling the continuing professional development requirements of their State or Territory (i.e. so you are not considered negligent in your area of practice including maintaining physical filing, storage, cyber and computing infrastructure in a way that exceeds or, at minimum, complies with industry standard and government laws and standards (i.e. so you are not negligent in your obligations in collection and holding of personal data).

Poorly maintained cyber security within a law firm means the practice is vulnerable to hacking, theft or misuse of information which may result in statutory penalties, lawsuits, and irreparable reputational harm.

Legal practices that have successfully remained largely paper-based have the same duty of care as those who have embraced information technology and data back-ups to hardware or 'the cloud' (hardware you don't see). For paper-based legal practices, there are different measures required. Having an off-site storage facility is not a definitive answer unless that facility has its own adequate security. Having on-site storage of paper files, without any duplicates or scanned copies held safely off-site, may not be sufficient to meet the duty of care in the case of fire or flood. Ensuring the practice insurance policy is adequate to protect the practitioner and the practice from liability for loss of data or cyber theft above and beyond the standard insurance policies covering professional indemnity or fixtures and fittings.

→

"Highly publicised cyber breaches involving conveyancing practitioners have highlighted the importance of maintaining robust cyber security controls and practices."[2]

Risk management

Much of meeting the demands of legal practice, complicated as it is by the need for internet safety, proper data/information practices, and respect for the requirements of privacy laws, will be satisfied by due diligence. For the busy practitioner, this involves having at least an awareness of the relevant obligations, performing risk management (or outsourcing it) and determining what the minimum effort/best approach for the practice is.

In litigation would your firm be able to affirmatively show that it met the minimum standards for:

1. Data security;
2. Client information security;
3. Software vulnerabilities;
4. Adequate employee computer/cyber training;
5. Cyber insurance;
6. Data breach response strategy; and
7. Mandatory data breach reporting.

Performing an initial risk management which includes cyber is a prudent business strategy in general. For legal practitioners it is essential because of the data we accumulate, our unique duty to the courts and due diligence to our clients.

The area of cyber law and litigation remains relatively untested in Australian courts; however the principles of privacy, client rights, duty of care and due diligence are well established. A court would balance what a practice did (positive actions to respect privacy laws, guidelines and so forth), failed to do (actions which a client or member of the public would reasonably expect to be done on their behalf), or were negligent in failing to do.

"Fidelity Fund Will Not Pay: Where client money is lost to a scam, the Fidelity Fund will not provide compensation, even if the funds were held in trust."[3]

In the context of all the freely available information, it would be challenging to argue that it was too hard, too costly or too time-consuming to have one's legal practice compliant with laws, policies and guidelines. It is parallel to the practice's own interests (economic, social, ethical) to know about, and implement, these fundamental cyber safety precautions because even with adequate cyber insurance (again not a well-tested area in Australia), the insurer may deny a claim where there was clearly a failure to implement proper cyber safety and, indeed, insurance policies, as this area matures, will likely require proof of basic risk assessment and/or practice policies.

Cyber safety is a fundamental component of modern legal practice—it is a business function akin to accounting and human resources.

Litigation and penalties – the exposure of law firms in Australia

In Australia there has so far been less litigation than presently occurs in the USA and in the UK. In these overseas jurisdictions data breach/cyber theft has led to breach of contract, negligence, and class actions. This is not to say that class actions and private law suits are not possible in Australia, and as discussed above, the only answer to litigation will be the diligent application of readily available basic cyber safety.

Aside from potentially devastating reputational loss, every, and any, breach of personal data/information has the potential to result in litigation above and beyond any Commonwealth and State/Territory law penalties. There is some case law jurisprudence in Australia for breach of confidence litigation, plain 'negligence' litigation and although Australia has not yet recognised a tort of privacy, Australia has previously adopted jurisprudence and case law from foreign jurisdictions as guidance. After the breach is not the time to test just how far your relationship with your partners/law firm extends in terms of shared liability, contributory negligence and vicarious and/or fiduciary liability.

Recommendations

1. Establish a base line for your legal practice - a stock take - of your software, data/information & technology practices;
2. Perform a risk management analysis of your cyber security (see free Australian Government Risk Assessment Tool below, Ref. 3);
3. Ensure the data/information (including trust account/banking) you collect from your clients conforms with the *Commonwealth Privacy Act 1988* and relevant state/territory legislation;
4. Ensure that your law firm insurance policy includes adequate cyber insurance specific to the data you collect and hold, this may require more than the mandatory professional indemnity insurance required by your state/territory law society or board;
5. Ensure that your practice complies with the National Data Breaches Scheme, relevant recommendations of the Law Council of Australia any further applicable State/Territory statutory obligations;
6. Refer to the Law Council of Australia and additional websites (cited over page) to ensure you have properly minimised your firm's and your own vulnerability to avoidable cyber pitfalls.
7. Understand that actively managing cyber risk means regularly reviewing your contracts and the practices of all the 3rd and Nth party vendors used by you and those who provide services to your practice and/or its clients. ■

About EJ

EJ Wise is Principal at Wise Law in Melbourne, providing specific and assured cyber law advice to law firms and legal professionals. Specialising in cyber law, privacy, technology, cyber stocktake, cyber risk assessment and cyber education. Wise Law provides strategic and operational consulting regarding cyber risk management and preparedness, incident/breach response, information governance, data privacy, government and internal investigations, e-discovery, records and information management, ethics and emerging technology/innovation.

www.wiselaw.com.au

1. Article modified for publication. For entire article please see: https://www.legalpracticeintelligence.com.au/wp-content/uploads/2017/04/Lawyers-Duty-in-Cyber-by-EJ-Wise.pdf (accessed April 2019).
2. Grant Feary, Deputy Director, Law Society of South Australia. Riskwatch. PEXA responds to cyber attacks. August 2018. Page 1. https://www.lawsocietysa.asn.au/PDF/AugustRiskwatch.pdf (accessed March 2019).
3. RPA News. Cybercrime: a growing threat to lawyers and clients. Bulletin No. 44. Issued June 2018. Victorian Legal Services Board + Commissioner. http://www.lsbc.vic.gov.au/documents/RPA_News_44_June_2018.pdf (accessed March 2019).

ADMISSIONS CEREMONY 11 DECEMBER 2018 SUPREME COURT OF THE NORTHERN TERRITORY

↑ In alphabetical order:

Caitlin Reanna Shervill, Cameron James Michael Jones, Casimir Loki Zichi-Woinarski, Harold Peter Hollingsworth, Kate Mairi Bremner, Kiran McLaren, Mark James Frederick Munnich, Melissa Anna Beasley, Michaela Anne Vaughan and Storm Francis Lawlor.

ADMISSIONS CEREMONY 5 MARCH 2019 SUPREME COURT OF THE NORTHERN TERRITORY

← Left to right:

Denita Nair
Matthew John Gardiner
Myles Brown
Samuel Hamilton Cashmore; and
Antoinette Kathryn Leahy

Also, admitted in the Alice Springs Supreme Court, Alecia Buchanan.