# *CYBER* DUTY OF CARE

## How to minimise cyber vulnerability in the practice of law

*"...if an organisation does not demonstrate a commitment to privacy, people will look for alternative suppliers, products, and services."*

Office of the Australian Information Commissioner
February 2018

## Debunking Cyber Fears

This article will help you quickly identify the areas in your law firm or legal practice which need regular review in order to **ensure you are compliant** with relevant laws, regulations, standards, and guidelines, as well as help you meet basic client expectations. You will find easy-to-read tools, recommendations, and resources.

The pace of development in modern legal practices is a reflection of societal norms, as well as the particular style of the practice owner(s).

In law, many of us fear "the cloud" or other modern technologies that replace traditional and 'reliable' paper files, books, and methods. 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. This is certainly evidenced by the new reporting being collated by the Office of the Australian Information Commissioner since the changes to the Commonwealth *Privacy Act 1988* in 2018 which showed that **the legal industry ranked third (out of the top five industry sectors that reported privacy breaches) in the quarter from 1 July - 30 September 2018**.

### So what?

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.

Your client's rights include ethical and safe handling of their information.

Legal clients and society reasonably expect that you as a practitioner are fulfilling the continuing professional development requirements of your State or Territory (i.e., so you are not considered negligent in your area of practice).

Legal clients and society expect you and your firm to maintain 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).

## What **is** my 'industry' [law firm] standard for cyber security?

In February of 2018, the Office of the Australian Information Commissioner released 'A Guide to Managing Data Breaches in Accordance with the Commonwealth *Privacy Act 1988*'. This guide provides easy to read information on how:

- the Privacy Act **applies to law practices**;
- the 2018 changes to the Privacy Act affect legal practices;
- to identify examples of breaches;
- to find information related to:
  - getting a greater understanding of the Privacy Act [Part 1 and Part 4 of the Guide];
  - preparing a data breach response strategy [Part 2 and Part 3 of the Guide];
  - how to respond to a data breach [Part 4 of the Guide – specifically the **mandatory data breach reporting and assessment requirements of the National Data Breaches (NDB) scheme].**

*...poorly maintained cyber security makes your practice vulnerable to hacking, theft or misuse of information which means you may be subject to statutory penalties and/or lawsuits (not to mention reputational*

Do you know if your practice meets the minimum standards for:

- data security
- client information security
- software vulnerabilities
- adequate employee computer / cyber training
- cyber insurance
- data breach response strategy
- mandatory data breach reporting

> Highly publicised cyber breaches involving conveyancing practitioners have highlighted the importance of maintaining robust cyber security controls and practices.
>
> Law Society of South Australia

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 - what if there is fire or flood? Does the practice insurance policy cover liability for loss of personal data or cyber theft above and beyond the standard policy cover for bricks and mortar/fixtures and fittings?

# 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 your due diligence. For the busy practitioner, this involves ensuring you have at least an awareness of your obligations, are performing risk management (or having it performed for you) and are determining what your minimum effort / best approach for your practice is.

## WHY PERFORM YOUR OWN RISK MANAGEMENT

**LIABILITY**

**PRACTICALITY**

**BEST PRACTICE**

**FINANCIAL SURETY**

A pragmatic legal practitioner might ask 'well, what can I get away with?' 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.

A court would look at what information was easily and practically available for the practice (see reference list below, a large amount of which is free). A court would most likely consider whether the practice had:

- performed its own risk assessment & managed accordingly;
- appointed person(s) to be responsible for managing data/information/privacy/technology within the practice;
- conformed with the relevant practice guidelines on cyber from bodies such as the Law Council of Australia, the Law Society NT, the Australian Cyber Security Centre's 'Stay Smart Online', the Australian Government Department of Industry, Innovation & Science's business, and the Office of the Australian Information Commissioner; and
- adequately discharged their basic duty of care.

**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.

Victorian Legal Services Board + Commissioner

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. Furthermore, larger clients will require some level of coverage for cyber perils (thus triggering due diligence to determine premium costs).

## I am resource and time poor

Even the briefest risk assessment will reveal that this is not window dressing. Weighing the relatively low investment of time and money into decent cyber safety against the high loss/high risk outcome of having inadequate cyber safety. The practice investment into cyber safety is elementary.

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

Confidentiality is the heart of our business – both ethically and practically.

Queensland Law Society

Cyber safety is a fundamental component of modern legal practice.

## what kind of penalties or litigation could I, or my firm, be exposed to if I opt to do nothing?

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. My advice: do not be the legal practice 'cyber-fail' test case for Australia. 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 below) 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 THE AUTHOR

EJ Wise is Principal at Wise Law in Melbourne.

## REFERENCES

1. Commonwealth *Privacy Act 1988*. Compilation No. 79. Compilation date 6 Nov 18. http://classic.austlii.edu.au/au/legis/cth/consol_act/pa1988108/ (accessed Mar 2019).

2. Stay Smart Online. Small Business 'Protect Your Business in 5 Minutes' 2nd edition. Stay Smart Online. Canberra: 2017. https://www.staysmartonline.gov.au/sites/default/files/Stay-Smart-Online-Small-Business-Guide_1.pdf (accessed Mar 2019).

3. Legal Practitioners' Liability Committee. Cyber Security. http://lca.lawcouncil.asn.au/lawcouncil/cyber-precedent-home (accessed Mar 2019).

4. Law Institute of Victoria. Cyber Security Essentials for Law Firms. 2017. https://www.liv.asn.au/getattachment/Professional-Practice/Areas-of-Law/Technology-and-the-Law/Resources/20171122_LP_LawTechEssentials_CyberSecuirtyFirms-v02.pdf.aspx (accessed Mar 2019).

5. Law Institute of Victoria. Cyber Security Essentials for the individual. 2017. https://www.liv.asn.au/getattachment/Professional-Practice/Areas-of-Law/Technology-and-the-Law/Resources/20170817_LP_LawTechEssentials_CyberSecurityIndividual_V04.pdf.aspx (accessed Mar 2019).

6. Law Institute Journal. Notifiable Data Breaches: It's complicated. Fabian Horton. 2018. https://www.liv.asn.au/Staying-Informed/LIJ/LIJ/March-2018/Notifiable-data-breaches--it%E2%80%99s-complicated# (accessed Mar 2019).

7. Victorian Legal Services Board + Commissioner. RPA News. Cybercrime: a growing threat to lawyers and clients. 2018. http://www.lsbc.vic.gov.au/documents/RPA_News_44_June_2018.pdf (accessed Mar 2019).

8. Queensland Law Society. Cyber Security. http://www.qls.com.au/Knowledge_centre/Ethics/Resources/Cyber_security (accessed Mar 2019).

9. Australian Cyber Security Centre. https://cyber.gov.au/business/ (accessed Mar 2019).

10. Australian Office of the Information Commissioner. Data Breach Preparation and Response Guide. 2018. https://www.oaic.gov.au/agencies-and-organisations/guides/data-breach-preparation-and-response (accessed Mar 2019).

11. Australian Competition and Consumer Commission. https://www.accc.gov.au/business/business-rights-protections/avoiding-scams (accessed Mar 2019).

12. Australian Government Department of Industry, Innovation & Science. Cyber Security risk assessment tool. Canberra: November 2018. https://www.business.gov.au/centre-for-defence-industry-capability/resources/useful-cyber-security-resources (accessed Mar 2019).

13. Australian CyberCrime Online Reporting Network (ACORN). https://www.acorn.gov.au/ (accessed Mar 2019).

14. International Organization for Standardization. Information technology — Security techniques — Cybersecurity and ISO and IEC Standards. ISO/IEC TR 27103:2018 (accessed Mar 2019).

15. International Organization for Standardization. Information technology - Information Security Management Systems. ISO/IEC TR 27001:2013 (accessed Mar 2019).

16. International Organization for Standardization. Information technology - Guidelines for Cybersecurity. ISO/IEC TR 27032:2012 (accessed Mar 2019).