Managing cyber risk – practical guidance

Simone Herbert-Lowe is a senior claims solicitor at Lawcover.

Lawcover

By Simone Herbert-Lowe

With the incidence of cyber-crime growing, a law practice needs to consider both risk management and risk transfer (through cyber risk insurance) when assessing a response to cyber risk.

While there are no specific rules regarding the steps that each law practice should take, it is important to remember that solicitors are custodians of confidential information. It may be difficult to defend a claim relating to a cyber breach where fundamental protection measures are not in place.

Snapshot

- Managing cyber risk is now an integral part of legal practice.
- Lawcover has purchased a group cyber risk insurance policy for its insured law practices which takes effect from 1 January 2018 and includes crisis assistance when a cyber event occurs.
- It is prudent for a law practice to consider both risk management and risk transfer when considering a response to cyber risk.

Law practices should consider the following guidance when looking to manage cyber related risks:

Software and virus protection

- Ensure that adequate business security software is used;
- Ensure that up-to-date antivirus protection is in place;
- Complete regular data back-ups.

Payment processes

- Record payment instructions at the commencement of a matter;
- Use validation checks when payment directions are changed.

Staff awareness and training

- Incorporate appropriate policies and staff training;
- Ensure that passwords are unique and changed regularly;
- Ensure you and your staff are conscious of the risks of:
  - clicking on suspicious attachments or hyperlinks in emails;
  - using free or unsecured WiFi;
  - importing material onto your network through a USB;
  - taking confidential material outside the workplace via USB-mobile phone or laptop;
  - sending confidential information by unencrypted text messages.
- Set up appropriate security checks and procedures for visitors to your workplace, particularly those engaged in upgrading software or computer networks.

Plan ahead

- Have an emergency respose plan if your network is disabled.

Data security

The Federal government has introduced the Notifiable Data Breach Scheme under the *Privacy Act 1988*. The scheme will apply to:

- Australian Government agencies and contractors that provide services for those agencies;
- all businesses and not-for-profit organisations with an annual turnover of more than $3 million;
- health service providers and holders of health records;
- credit reporting agencies; and
- organisations holding individual's tax file numbers, which are subject to the legislation for the purpose of those records.

Any entity that receives a tax file number ('**TFN**') of an individual is classified as a 'file number recipient' and must not record, collect, use or disclose TFN information unless permitted to do so by law.

The reporting obligations come into effect in February 2018. They require the reporting of breaches to both the affected person and the Office of the Australian Information Commissioner, if there has been a privacy breach that could lead to 'serious harm'. The term 'serious harm' is not defined in the Act, however the Act does provide a list of relevant matters that organisations should consider when assessing whether a breach would or would not be likely to result in serious harm. Notification is a mandatory requirement of the regime and there are penalties for non-compliance.

For more information about the Notifiable Data Breach Scheme, see: Nick Abrahams and Jamie Griffin 'The end of a long road: Mandatory data breach notification becomes law' 32 *The Law Society of NSW Journal*, April 2017, 76-77; Helen Brown 'Is your practice secure? Client confidentiality and data breach' 39 *The Law Society of NSW Journal*, November 2017, 88-89; Michelle Meares 'Mass surveillance and data retention: do the means justify the ends?' 40 *The Law Society of NSW Journal*, December 2017, 76-77.

Crisis assistance and insurance

Lawcover has purchased a group cyber risk insurance policy from Barbican Insurance which provides foundational cyber risk cover to Lawcover insured practices. Commencing on **1 January 2018**, the policy includes access to an incident response team for assistance in the event your computers or computer network are disabled.

For crisis assistance relating to a cyber event contact:
Phone: 1800 273 224
Email: lawcyber@cbp.com.au **LSJ**