Law Council OF AUSTRALIA
Legal Practice Section
AUSTRALASIAN Law Management Journal

Edition: January 2020

The insurance jigsaw puzzle – how different policies respond to cyber events and email fraud

Lawyers face more risks that most professionals because of their duties around managing money held in trust, so it is essential that firms understand their particular threats and take out appropriate insurance cover that can protect them from malicious attacks, writes Simone Herbert-Lowe.

Snapshot:

- Lawyers' professional indemnity policies usually provide broad coverage for third-party claims, but not for a firm's own losses.
- Cyber insurance can offer additional types of cover, including specialist technical support to assist in responding to a cyber event.
- Three types of insurance – professional indemnity insurance (PII), cyber and crime cover – may be required for comprehensive protection.

A recent Allianz global survey of risk managers reported that for the first time cyber incidents were regarded as the top peril for companies.

For professionals, including lawyers, with special duties of confidentiality and fiduciary obligations to manage money held in trust, the risks may be even greater. In a recent study of 172 Australian and New Zealand law firms by ALPMA and GlobalX, 87 per cent of respondents indicated cybersecurity was a concern and almost one in five respondents reported a cybersecurity breach at their firm in the past two years – with this figure jumping to almost 40 per cent for firms of between 75-149 employees.

Risk prevention includes implementing technical cybersecurity measures, staff education and appropriate risk-management processes. But if, despite those measures, your firm is the victim of a cyber incident or email fraud, will you be covered under your insurance?

Law Council OF AUSTRALIA
Legal Practice Section
AUSTRALASIAN Law Management Journal

Insurance cover

When it comes to the potential impact of cyber events and email fraud on legal practices, three different types of policies may be required for comprehensive insurance cover – professional indemnity insurance (PII), cyber-risk insurance and crime cover designed to respond to electronic funds transfer frauds. While policy wordings vary significantly, and should be carefully considered before making insurance decisions, the following general overview explains how different classes of insurance can support your firm's cyber-resilience strategy.*

Third-party losses

Third-party claims are usually made by clients and former clients, but they can be made by non-clients, such as beneficiaries under a deceased estate. **PII** policies for legal practices generally provide broad coverage for third-party claims. If, for example, a client brings a claim against your firm for paying money into the wrong bank account as a result of an email scam in which you were given false bank account details for your client, then your PII policy is most likely to respond to any claim by the client against the firm.

However, where cyber fraud or email scams involve the loss of the practice's own funds, a policy designed to cover only third-party claims is unlikely to respond. The practice would likely be uninsured for this loss, unless it had purchased a suitably worded crime policy or crime cover included under another policy.

Firm losses

Business email compromise involving impersonation fraud often involves firms' own money. A typical example is known as 'CEO fraud' and involves a fake email that appears to be sent by a managing partner to someone in the firm's accounts department.

If the accounts officer fails to detect the scam and actions the payment requested in the fake email, the money is likely to become untraceable within a short period. **Crime policies**, or crime cover included in other relevant policies (such as management liability or comprehensive cyber-risk policies) can provide cover for electronic crimes, including funds transfer frauds as a result of business email compromise, but it's prudent to check these to ensure that electronic funds transfer frauds and social engineering/impersonation fraud are expressly included.

Cyber events involving computer intrusion through ransomware or hacking can require urgent responses to contain damage, loss and disclosure of client information. The ability to access specialist IT support at a time of crisis is an important feature of cyber insurance. For example, IT experts who specialise in responding to cyber events hold keys that unlock

malware, and are experienced in quickly identifying evidence of and responding to system breaches.

Cyber-risk policies generally offer this type of crisis assistance, which provides significant support in limiting the firm's own business losses through proactive, early intervention. There are a range of policies for law firms to consider, each offering a different suite of coverages. Policies that are foundational in nature focus on coverage such as technical assistance in the case of a cyber event, defence costs and penalties for regulatory investigations, business interruption costs and cyber extortion payments.

Policies designed to offer more comprehensive protection can include other types of cover such as comprehensive computer crime cover, reimbursement for costs associated with responding to fraudulent electronic communications impersonating your business, and a range of other exposures.

Most importantly, lawyers should consider their individual practice needs when considering insurance for cyber events – *before* they occur.

Simone Herbert-Lowe is the solicitor director of Law & Cyber, which provides legal advice, risk-management services and online cyber-resilience education for professionals.

* This article provides a general overview of how different types of insurance policies might respond to cyber events. However, policy wordings vary across jurisdictions, insurers and policies, so you should check your own policies to assess the insurance cover presently available to your firm. This article provides general information only and does not constitute legal or insurance advice. If you require such advice, you should seek specific advice tailored to your circumstances.