The hidden cost of cyber neglect

Risk Management Topic:

Cyber Security

Candice Perriman
Risk Education Manager

Cyber attacks are a pervasive risk that every practice must actively manage. From business email compromise to ransomware, cyber threats are increasing in frequency, sophistication and impact. For a profession built on confidentiality, trust and compliance, the consequences of a cyber breach for a law practice can be severe.

Recent threat intelligence

The Australian Signals Directorate's Annual Cyber Threat Report 2024–25 (ASD Report) reveals a sharp rise in cyber crime across all sectors, with the professional services sector (including law practices) among the most affected. The Australian Signals Directorate (ASD) received over 84,700 cyber crime reports in the past year, an average of one report every 6 minutes.

Ransomware and data breaches

According to the ASD Report, threats such as ransomware and data breaches are on the rise, with cyber criminals using stolen credentials to compromise networks.

Law practice example: Cyber criminals infiltrate a law practice's system to monitor emails, intercept messages and send fake bank details, redirecting funds to their own account.

Credential theft

Credential theft continues to be a major tactic, with stolen usernames and passwords used to access personal and corporate accounts.

Law practice example: Cyber criminals steal law practice account credentials (e.g. online banking login details) through phishing or malware and infiltrate systems, accounts, apps, etc.

Outdated systems and poor logging practices

Outdated systems and poor logging practices remain a vulnerability. Law practices are exposed if they are using outdated infrastructure with insufficient logging activities, to support effective detection of unauthorised access.

Law practice example: The law practice uses an outdated document management system that hasn't received security patches in over a year. A cyber criminal scans for vulnerabilities, finds an unpatched flaw and exploits this to gain initial access. Without detailed logs, the practice can't see who has accessed sensitive information, when or from where. The loss and damage experienced by the law practice increases because logging has not flagged the initial breach.

The hidden cost of cyber neglect

Managing the risk

Law practices are custodians of clients' trust information and funds. A cyber incident can jeopardise client relationships, disrupt operations, breach ethical obligations, and trigger legal liability. The financial impact can be significant. The ASD Report shows that the average cost for small, medium and large businesses (including law firms) is $80,850 per incident – a 50% increase from the previous year.

To help law practices mitigate cyber risks, Lawcover has developed a range of cyber resources tailored for law practices, including a comprehensive Cyber Security Guide and Step by Step Instructions detailing the measures you should take to keep your practice and your clients safe.

At a minimum, law practices should:

– **Enforce multi-factor authentication across all systems**

– **Use strong, unique passwords and secure password managers**

– **Keep software and systems up to date**

– **Train staff to recognise phishing and social engineering**

– **Regularly back up data and test recovery plans**