Quick cautionary tales for a better practice

Episode 78

Beyond Third Party Advice

In *Australian Information Commissioner v Australian Clinical Labs*, Australian Clinical Labs suffered a cyberattack on IT assets it had acquired a few months earlier. A malicious actor had encrypted files and issued a ransomware demand. The company engaged a third party consultant, who initially assessed the threat as a scare tactic and suggested that the removal of sensitive data was unlikely.

The company did not notify the Privacy Commissioner of the breach. Then, a few months later the Australian Cyber Security Centre confirmed that a large volume of highly sensitive personal data including passport details and financial information had been exposed on the dark web.

As a result, the Australian Information Commissioner commenced proceedings against the company for failing to take reasonable steps to protect individuals' personal information from unauthorised access.

In the decision the court was critical of the company's initial response following the cyberattack. Key members of staff initially put in charge of the response had received no training in how to respond to a cyberattack and were largely dependent upon advice provided to them by a third party provider. The company was ordered to pay $5.8 million in civil penalties, marking the first time a regulated entity has faced such penalties under the Privacy Act. This is a strong reminder that serious failures to safeguard personal information held by entities can have significant consequences.

For law practices, even though third party providers can be valuable partners in managing cyber threats, the ultimate responsibility for safeguarding client and personal information rests with the practice. Regulators expect entities to take proactive steps to ensure systems remain secure and that breaches are reported in line with legal obligations. Relying solely on external advice without internal capability or oversight can leave your practice exposed to significant penalties and reputational damage.

Legal practices should:

- Educate and train staff on cyber incident response plans and test these plans regularly
- Maintain internal capabilities to validate advice and make informed decisions
- Avoid over-reliance on third parties and assign trained staff to lead responses, not just external providers
- Ensure understanding of and compliance with the Privacy Act, including obligations to notify an 'eligible data breach'

I'm Malcolm Heath

Australian Information Commissioner v Australian Clinical Labs Limited (No 2) [2025] FCA 1224