On notice

Lessons from *ASIC v RI Advice Group Pty Ltd*

Cyber attacks are one of the most prominent threats that businesses face today. The recent Federal Court judgement in *Australian Securities and Investments Commission v RI Advice Group Pty Ltd [2022] FCA 496* emphasises the importance of all businesses investing in robust, cyber security risk management systems and practices.

Background

Australian Financial Services licensee, RI Advice Group Pty Ltd (RI), experienced a number of cyber security incidents between 2014 and 2020 including:

- Unauthorised access to RI's server and installation of malicious software which compromised the personal information of thousands of clients
- Hacking and impersonation of staff email accounts resulting in clients receiving fraudulent emails requesting bank transfers
- Ransomware attacks resulting in the encryption of client information which was then unable to be recovered.

The Federal Court found that RI had breached its licence obligations by failing to implement adequate cyber security risk management systems and ensure cyber resilience. RI was ordered to pay $750,000 towards ASIC's costs and, at its own expense, engage a cyber security expert to identify and implement any necessary cyber security measures.

In handing down her decision, Justice Rofe noted that *"cyber security risk forms a significant risk connected with the conduct of the business and the provision of financial services".*

While it is not possible to reduce cyber security risk to zero, her honour said it was *"possible to materially reduce cyber security risks through adequate cyber security documentation and controls to an acceptable level".*

Implications

While this case involved an Australian Financial Services licensee, the broader message is clear.

Increasing obligations are being placed on businesses, particularly those holding sensitive and confidential information. Cyber security and resilience must be an integral part of a law practice's risk management strategy. Appropriate steps need to be taken to ensure that adequate measures, processes and procedures are in place including:

- Having a cyber incident response plan in place
- Scheduling regular data backups and regularly testing the integrity of those backups
- Using a Virtual Private Network (VPN) to ensure a safe internet connection
- Ensuring mobile devices are regularly updated and backed up
- Setting up multifactor authentication for all devices.

Cyber security is a complex issue. Although cyber breaches can never be completely eradicated, they can be minimised through proper risk management.

Lawcover has developed a number of practical resources specifically tailored to help guide legal practitioners in cyber risk management.

For guidance see:

- Lawcover cyber resources
- *Australian Securities and Investments Commission v RI Advice Group Pty Ltd [2022] FCA 496*