HOWDEN | Hall&Wilcox smarter law

Cyber risk in Australia's professional service sector: a growing threat

Cyber risk in Australia's professional services sector: a growing threat

Australia's professional services sector continues to undergo a seismic shift. Legal, accounting, and consulting firms are embracing digital tools to streamline operations, enhance client service, and stay competitive. But with innovation comes exposure.

Firms that digitise their workflows are not just improving efficiency – they're also expanding their attack surface. Cyber criminals are watching closely and targeting the very assets that make these firms so valuable: sensitive client data, financial records, and trust.

Ransomware and data breaches are increasingly the enemies of enterprise for Australia's professional services sector. Cyberattacks are no longer just about locking up systems: it's about stealing sensitive data, exposing confidential client information, and weaponising reputational damage. Firms, particularly those uninsured and without robust incident response plans, are being forced into high-stakes decisions under immense pressure, often with little time or access to experts to respond.

The Australian Cyber Security Centre (ACSC) and the Office of the Australian Information Commissioner (OAIC) continue to issue urgent guidance, warning that without proactive cyber and privacy risk management, firms risk becoming the next cautionary tale. A breach isn't just a technical failure; it's a business-defining crisis.

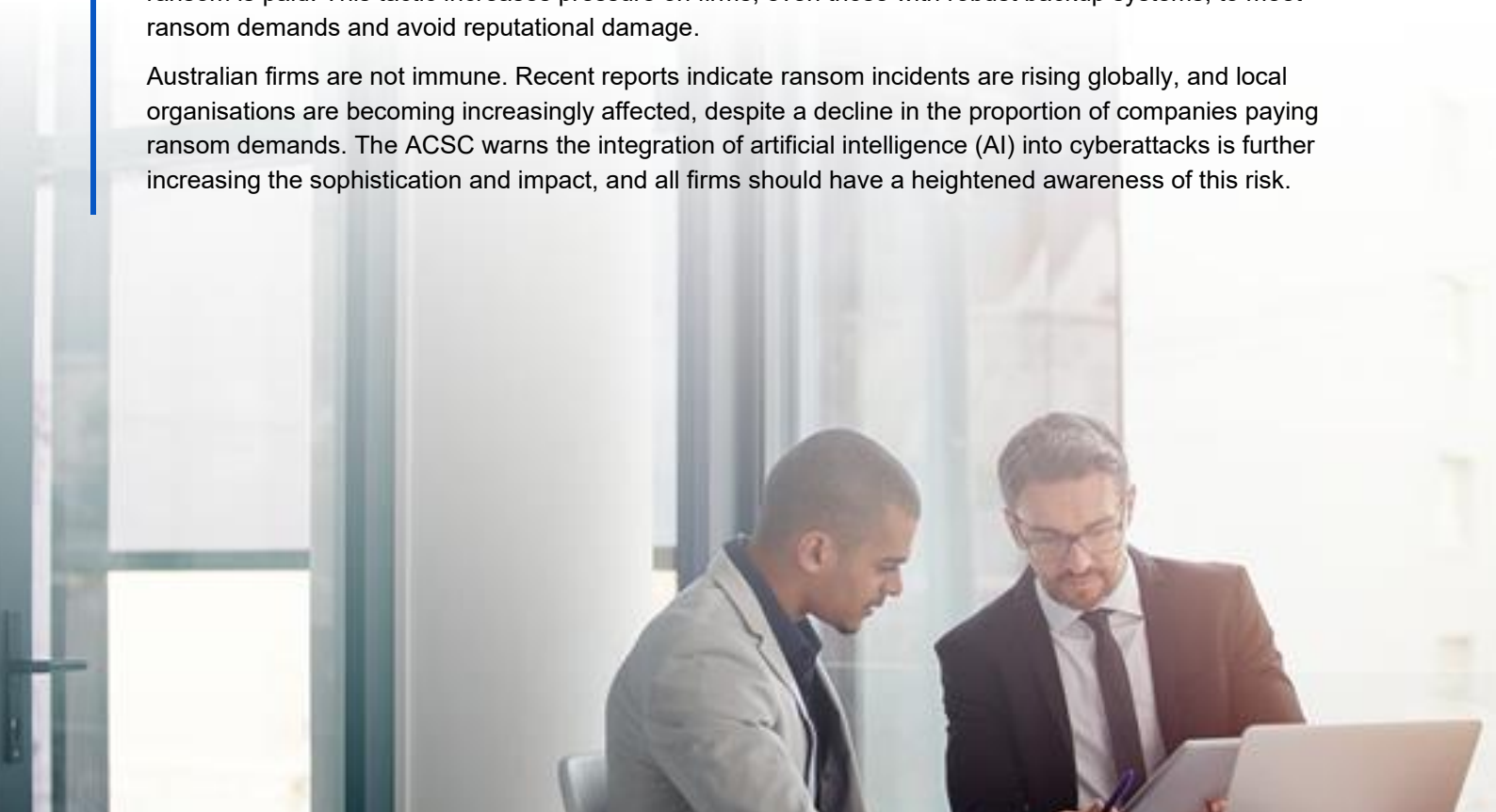
It's imperative that businesses take appropriate steps to arm against this growing threat. Investing in cyber insurance offers a critical safeguard, by helping mitigate financial and regulatory risks and offering access to expert resources if an incident occurs.

Ransomware: a pervasive threat in Australia

Ransomware attacks have evolved beyond simple data encryption.

Attackers often exfiltrate sensitive data before encrypting systems, threatening to publish it online unless a ransom is paid. This tactic increases pressure on firms, even those with robust backup systems, to meet ransom demands and avoid reputational damage.

Australian firms are not immune. Recent reports indicate ransom incidents are rising globally, and local organisations are becoming increasingly affected, despite a decline in the proportion of companies paying ransom demands. The ACSC warns the integration of artificial intelligence (AI) into cyberattacks is further increasing the sophistication and impact, and all firms should have a heightened awareness of this risk.



Case study: the value of cyber insurance

Imagine this: it's Friday morning at an accounting firm. Staff log in, ready to tackle client deadlines, only to find every system is frozen. Emails won't send. Files won't open. Even the backups are locked. A chilling message appears…

> Pay the ransom or lose everything.

This isn't fiction. It's the reality of a ransomware attack. In this case, the firm's entire digital infrastructure was encrypted, including sensitive client records and financial data. The clock was ticking, and operations were at a standstill.

Fortunately, the firm had cyber insurance. Within minutes, a specialised incident response team was activated. They assessed the damage, negotiated with the attackers, and began the process of restoring systems. Within 48 hours, the firm was back online. This outcome may be rare, but possible with the right preparation and response.

But not every firm is this lucky. Recovery can take weeks. The reputational damage can linger for years. The critical truth is that cyber risk isn't just technical, it's existential. Without a response plan and the right insurance coverage, a single breach can unravel years of trust and progress.

This has unfortunately been the case for many organisations. While it is difficult to meaningfully quantify the financial impact of ransomware attacks on a business, without individual isolation, it is not uncommon for the costs of a ransomware incident to exceed half a million dollars in first party costs. This is before accounting for business interruption and third-party claims.

These figures highlight just how devastating a ransomware incident can be, extending far beyond immediate technical disruption to encompass significant financial and reputational harm. In this high-risk environment, cyber insurance is a vital safeguard, offering not only financial support but also access to expert resources when every second counts.

Cyber insurance can alleviate much of the financial burden by covering the following:

- Forensic investigation costs
- Professional advice, including legal and public relations
- Data restoration costs
- The costs of a ransom negotiator
- The ransom payment itself; business interruption losses, sometimes including losses from reputational harm
- Defence costs for third-party claims

The consequences of a breach

Australia's privacy framework has undergone significant reform, raising the stakes for professional services firms handling personal information.

Regulatory risks	*The Privacy Act 1988 (Cth)* now contains expanded enforcement powers for regulators, including the OAIC. These powers include the ability to: • Impose infringement notices for administrative-style breaches of the Privacy Act, up to a maximum of $19,800 for a body corporate or $66,000 for a publicly listed company. • Issue compliance notices requiring entities to do, or refrain from doing, certain acts to address privacy contraventions. • Commence legal proceedings for low to mid-range privacy interferences, with a maximum penalty of $3.3 million per contravention. • Commence legal proceedings for serious breaches, with a maximum penalty of at least $50 million per contravention. We expect the broader range of enforcement powers will heighten regulatory risk overall. The OAIC is not the only regulator with a sharpening focus on cyber and privacy incidents. ASIC (Australian Securities and Investments Commission) and APRA (Australian Prudential Regulation Authority) have both indicated they expect businesses to take their cyber security obligations seriously and will carefully scrutinise any incident that comes to their attention. Incidents need to be carefully managed to address these risks, with ongoing, timely legal and professional advice being essential. These legal risks further underscore the importance of insurance.
Third-party legal risks	Recent reforms to the Privacy Act have also introduced a statutory tort for serious invasions of privacy, allowing individuals to bring proceedings directly against businesses who recklessly or intentionally interfere with their privacy. This tort has not yet been tested by a court, and we expect this uncertainty to encourage potential plaintiffs to test the scope of the tort. This means firms now face not only regulatory penalties, but also civil litigation risks that may involve further legal expenditure or civil damages. The introduction of the tort, along with the nature of the Australian legal landscape, makes privacy a ripe vehicle for class action plaintiff firms. Australia has already seen the first wave of class actions arising from cyber incidents and it is reasonable to expect the number of class actions to increase in coming years.
Other risks	A growing risk for businesses is the reputational damage associated with data breaches, particularly where a business fails to take all reasonable steps to address the breach. Recent market research by Hall & Wilcox shows that organisations who provide prompt, comprehensive and accessible information to impacted individuals increase trust and improve consumer loyalty. A company's ability to provide information in this manner is strongly supported by a network of appropriate service providers: a key benefit available through a cyber insurance policy.

Establishing a cyber security toolkit

To remain compliant, resilient, and insurable, Australian professional services firms should adopt a two-pronged approach:

1 Strengthen privacy governance

2 Implement core cyber security controls

Privacy governance essentials

- Regularly review and update privacy policies.
- Undertake data mapping and assess data retention obligations.
- Implement breach detection and response procedures.
- Train staff on privacy obligations and data handling.
- Audit information handling practices and third-party contracts.
- Conduct regular penetration testing, identifying weaknesses before they are exploited.

Privacy compliance is a strategic imperative, not just a legal requirement.

Essential cyber security controls

To safeguard sensitive data, reduce cyber risk, and meet insurance requirements, firms should prioritise the following measures:

Invest in people: run annual cyber awareness training and phishing simulations to turn staff into your first line of defence. People can be your greatest asset.

Enable Multi-Factor Authentication (MFA): add an extra layer of security to remote access, admin accounts, and email.

Maintain secure data backups: encrypt, store offline and test restoration regularly to ensure business continuity.

Test, enhance, and review business continuity and incident response plans: be prepared to respond quickly and minimise downtime when an incident occurs.

Filter emails effectively: block malicious links and attachments before they reach inboxes.

Enforce a patch management policy: apply critical updates as soon as possible to close security gaps.

Strengthen password management: use strong, unique passwords and secure management tools.

Deploy advanced endpoint protection: keep devices safe with up-to-date antivirus and firewalls.

Isolate end-of-life systems: segregate outdated systems from active networks to reduce risk.

These controls aren't just best practice; they're the baseline expected by insurers, cybersecurity experts, and your customer base. Building a culture of cyber awareness across all levels of your organisation through regular staff training, clear incident response protocols, and active leadership engagement further strengthens your cyber security posture and reduce the likelihood of a breach.

Leadership teams and boards should use simulated table-top exercises to prepare for potential cyber incidents. These exercises run through the key decision points that arise during an incident. They are both good practice for decision makers and effective in identifying gaps that need strengthening.

Conclusion

Cyber risk is an immediate and escalating challenge for Australia's professional services sector.

By implementing robust cyber security measures and maintaining a proactive risk management strategy, firms can take steps to protect their reputation, financial stability, and client trust.

But firms can't assume that proactive preparation will solve everything. When (not if) things go wrong, an organisation's appropriate and timely response can be critical to its very existence. It's in these cases where the support of a cyber insurer, and a network of appropriate professionals who understand the challenges your business faces, will be invaluable in responding to a crisis.

> **For professional services firms across the Pacific, cyber risk isn't a question of if, but when.** The real differentiator isn't just having security controls in place; it's building resilience and having the ability to respond quickly when the inevitable happens. Why does this matter? Because globally, cyber incidents cost the economy 40 times more than fire-related risks and for firms built on trust, the cost of inaction is even higher."
>
> Jack Bassett
> **Senior Associate, Cyber & Technology Solutions, Howden**

> **Cyber risk is one of the greatest risks of our time.** Cyber incidents can have a material impact on the financial wellbeing and reputation of professional service firms. Cyber insurance forms an important part of the overall risk management approach that professional service firms should be considering."
>
> Eden Winokur
> **Partner and Head of Cyber, Hall & Wilcox**

Talk to us today.

Jack Bassett
Senior Associate, Cyber & Technology Solutions
Howden

T +61 428 977 730

E jack.bassett@howdengroup.com

Eden Winokur
Partner and Head of Cyber
Hall & Wilcox

T +61 2 8267 3257

E eden.winokur@hallandwilcox.com.au

www.howdeninsurance.com.au