



Client Advisory

Don't make it easy for them – understanding cyber risk in 2026

Cyber risk has become a business risk

Cyber threats continue to evolve rapidly, affecting organisations of every size, industry and geography. New Zealand incidents such as the Manage My Health and ZenTech breaches show the operational, financial and reputational consequences that can follow.

Cyber criminals are not only targeting large enterprises. Atmos Intelligence data indicates that more than 80% of identified incidents involve small and medium-sized organisations ('SMEs'), with small businesses accounting for over 60% of those impacted. Often seen as easier targets, SMEs may also provide pathways into larger customers and supply chains.

Cyber risk is therefore not solely an IT issue. It is a governance, operational, financial and reputational risk that business leaders must actively manage.

What are we seeing in the current cyber threat landscape?

Many incidents still begin with relatively simple methods that exploit human behaviour or common technical weaknesses, including:

- Business Email Compromise (BEC) and invoice fraud
- Ransomware and double-extortion attacks
- Exploitation of unpatched and zero-day vulnerabilities
- Third-party and supply chain compromise

Double-extortion ransomware has intensified the impact of attacks. Threat actors steal sensitive information before encrypting systems, then threaten to publish or sell it if demands are not met.

Cyber criminals also exploit unpatched and newly discovered "zero-day" vulnerabilities, scanning exposed systems and gaining access before critical updates can be applied.



Client Advisory

How are cyber criminals getting in?

Understanding common entry points is an important first step towards improving cyber resilience.

Business email compromise

Fraudulent emails impersonate trusted people or organisations, enticing users to open attachments, disclose credentials or follow malicious links. AI is making these attacks more convincing and effective.

Exploitation of vulnerabilities

Attackers use automated tools to exploit unpatched and newly discovered vulnerabilities, access systems, steal data and deploy ransomware.

Third-party & supply chain compromise

Compromised suppliers, software providers and service partners can provide threat actors with a trusted pathway into customer systems and sensitive information.

What does cyber insurance cover?

While strong security controls are essential, no organisation can completely eliminate cyber risk. Cyber insurance is designed to assist businesses in responding to and recovering from cyber incidents by providing access to specialist support and financial protection.

Cyber insurance supports incident response and recovery through specialist expertise and financial protection. Subject to policy terms and conditions, cover may include:

- Incident response and forensic investigations
- Data breach response and notification costs
- Legal advice and regulatory investigations
- Cyber extortion and ransomware events
- Business interruption losses
- Public relations and crisis communications

A broader approach to cyber risk

Cyber resilience is most effective when organisations adopt a holistic approach that combines security, governance, and risk transfer. Cyber insurance is not a substitute for cyber security. It is one part of a broader strategy combining prevention, response and



Client Advisory

recovery. Together, ICIB and our cyber security partner Nectar believe cyber resilience is built on three core pillars:

1. Risk identification

Understanding your cyber exposure starts with an honest picture of what you actually have, not what you assume. That means knowing:

- What devices, accounts, and third-party services touch your business
- Where sensitive data really lives and where the gaps are
- System patches
- Strength of passwords
- Multi-factor authentication
- Monitoring

For most SMEs this picture doesn't exist until someone goes looking for it. A proper risk assessment turns assumptions into a prioritised list of exposures, so security spend goes toward what's most likely to cause a breach or a claim, rather than whatever feels most urgent that week.

2. Risk mitigation

Once the gaps are known, mitigation means closing them with practical, proven controls: multi-factor authentication on every account, a managed patching programme, 24/7 monitoring and response so an intrusion is caught in minutes rather than months, and tested backups kept separate from the main network. Staff training matters just as much as the technology, since most attacks still start with a person rather than a system.

Increasingly, businesses also want a way to prove this work is being done — to insurers, customers and their own boards. SMB1001 is New Zealand's cyber security standard for SMEs, and its Gold tier maps closely to the controls above. Achieving it gives a business, and its insurer, independent evidence that its cyber hygiene is more than a policy on paper.

3. Risk transfer

Using appropriate cyber insurance to protect the business from potentially significant financial consequences.



Client Advisory

Together, insurance expertise and cyber security advice provide a fuller view of the organisation's risk profile and the practical options available to reduce it.

Conclusion

Cyber criminals continue to seek organisations that are easiest to compromise. Although the threat landscape evolves, many attacks still exploit familiar weaknesses that can be addressed through sound governance, effective controls and ongoing vigilance.

Cyber resilience is a journey. Whether your organisation is beginning or maturing its programme, ICIB and Nectar can help identify risk, strengthen defences and prepare for recovery. Speak with us to review your current position and identify the next practical step for your business.

Questions or concerns?

For questions about your cyber risks or insurance cover, contact our Liability team -

liability@icib.co.nz
0800 644 444

Or speak with our cyber security partners at Nectar -

evolve@nectargroup.co.nz
0508 632 821