KINETICS GROUP

CYBER THREAT UPDATE

Q4 2025 | RAPID EXECUTIVE BRIEF

The 10-Minute Cyber Threat Intelligence Brief for Today's Business Leaders

About This Document

This quarterly briefing distils key cybersecurity developments and insights relevant to New Zealand business leaders. It is designed to inform Directors, CEOs, and Operations Managers of emerging risks, attack trends, and practical frameworks to strengthen organisational resilience. Prepared by Kinetics, this 10-minute read highlights actionable steps and proven strategies to help leaders make confident, informed decisions about cyber risk and governance.

Are You Still Feeling Lucky?

> ***A cybercriminal only has to be lucky once, while a defender has to be lucky every minute of every day.***
>
> **Combating Ransomware: A Comprehensive Framework for Action**
> US Department of Justice Task Force

Cybercrime is a global enterprise worth billions of dollars. The cost and complexity of defending against it continue to escalate, and absolute protection is no longer possible. The real question boards are asking is not "can we stop every attack?" but "are we doing enough to reduce our exposure and recover quickly when it happens?"

The answer lies in readiness, not luck. Effective governance requires consistent investment in people, policy, and platforms that can withstand today's fast-moving digital threats.

The New Zealand Threat Landscape 2025

New Zealand continues to face a growing number of cyber incidents across both public and private sectors. Law firms and real estate agencies continue to be targeted and key statistics from the National Cyber Security Centre (NCSC) show the scale and persistence of the threat:

Q1 2025 (January–March)	Q2 2025 (April–June)
1,369 Incidents reported	**1,315** Incidents reported
$7.8 m Direct financial losses, (14.7% increase from Q4 2024)	**$5.7 m** Direct financial losses
486 Scams and fraud cases, the most frequent category	**514** Scams and fraud cases, the most frequent category
440 Phishing and credential-harvesting incidents, the second most common	**> 50%** All reported losses affected businesses, not individuals
19 Incidents resulted in Operational Disruption	**16** Incidents resulted in Operational Disruption
10 Separate cases with losses exceeding $100,000	**22** Incidents resulted in Reputational Loss

> ***We encourage individuals and businesses to report incidents to us. The reports we receive help us build a clearer picture of the current threat environment and focus our efforts to protect New Zealanders online.***
>
> **Tom Roberts, Team Lead**
> NCSC Response & Investigations

Attacks Are Getting Faster

Artificial intelligence and automation now allow hackers to operate at machine speed to probe, test, and exploit vulnerabilities before most organisations even realise an attack has begun.

A lot can happen between your morning coffee and lunch.
Microsoft researchers recently analysed a Business Email Compromise (BEC) attack in which hackers set up a fake "typo-squatting" domain and infiltrated an active email thread within hours. By the time the business detected irregularities, confidential information had already been compromised.

Modern attacks unfold in hours, not days; leaving almost no room for human reaction.

What's at Stake?

Financial Impact
The ransom payment, if one occurs, is often the smallest cost. True financial losses include system restoration, downtime, legal and compliance expenses, lost revenue, and reputational damage. Adding to this challenge, two of the world's three largest reinsurers no longer cover ransomware payments, reflecting the rising frequency and severity of attacks.

Reputation and Trust
Reputational damage can far outlast operational disruption. When an organisation is found to have neglected reasonable precautions, it's not just the brand that suffers as leadership credibility and board reputation are also at risk.

Legal and Regulatory Exposure
Amendments to the Privacy Act 2020, which now align with the EU's GDPR, have increased obligations for protecting personal data. Failure to demonstrate "reasonable steps" to secure information may lead to investigation or prosecution under New Zealand law. Proactive compliance is now a business imperative, not an optional best practice.

Compliance Frameworks

Your Roadmap to Better Security

The two questions we hear most from business leaders are:

- "Where do we start?"
- "How do we know if we're doing enough?"

The good news is that you don't need to reinvent the wheel. Globally recognised cybersecurity frameworks offer proven pathways to establish structure, accountability, and measurable improvement.

CIS Critical Security Controls

The Center for Internet Security (CIS) Controls provide a prioritised set of 18 safeguards designed to defend against the most common attacks. Now in version 8.1, these controls are developed by a global community of cybersecurity experts.

Why CIS Controls Work for New Zealand Businesses

Prioritised approach
Controls are grouped into three Implementation Groups to match business size and resources:

→ IG1: Essential cyber hygiene for all organisations.
→ IG2: Enhanced security for multi-department or multi-site organisations.
→ IG3: Advanced protection for those managing highly sensitive data.

Prescriptive guidance
Clear, step-by-step actions replace vague policy statements.

Cost-effective
Foundational controls in IG1 deliver strong protection with limited investment.

Globally aligned
CIS maps directly to NIST, ISO 27001, PCI DSS, and HIPAA.

Cloud-ready
Version 8.1 addresses hybrid and cloud environments common in NZ.

Insurance recognition
Many cyber insurers acknowledge CIS compliance as a risk-reducing measure.

SMB1001 Standard

The SMB1001 standard was designed specifically for small and medium-sized businesses. Developed by Dynamic Standards International, it provides a staged, certification-based approach to building cybersecurity maturity.

Why SMB1001 Works for New Zealand Businesses

Designed for SMBs
Realistic steps that account for resource constraints.

Tiered certification
Bronze to Diamond levels let you progress as your business grows.

- → Bronze: Foundational controls (self-attested by Director)
- → Silver: Enhanced measures (self-attested)
- → Gold: Advanced practices (self-attested)
- → Platinum: Comprehensive security (externally audited)
- → Diamond: Highest level of maturity (externally audited)

Quick wins
Bronze requires just six essential controls, achievable in days.

International recognition
Certification demonstrates credibility with clients and insurers.

ISO 27001 alignment
Acts as a stepping stone to enterprise-level frameworks.

Regularly updated
Reviewed annually by public and private sector experts.

Insurance advantage
Some insurers now require Silver or Gold certification for cover.

Both CIS Controls and SMB1001 provide clear, structured approaches to cybersecurity maturity. Kinetics can help determine which framework best suits your organisation and guide you through its implementation.

Protecting Your Organisation

How Much Protection Is Enough?

Cybersecurity is an ongoing race between attackers and defenders. Defences that seemed excessive last year may already be outdated. Regular reviews of tools, processes, and training are essential to maintaining resilience.

> ***The cyber threats that Aotearoa New Zealand faces continue to evolve — more persistent, more sophisticated, and more capable of causing severe impact to service delivery and information security.***
>
> **GCSB Annual Report**
> 2024–2025

Timing Is Everything

Attackers are not waiting for you to be ready. They're testing your systems every day. Each failed attempt helps refine their next move. Strong defences don't guarantee immunity, but they do increase deterrence and reduce impact when a breach occurs.

Deterrence | Smarter Tools, Stronger Defences

Traditional antivirus is no longer sufficient. Modern environments require Endpoint Detection & Response (EDR); advanced systems that use behavioural analytics and machine learning to detect active threats, not just known signatures. EDR is now the global benchmark for effective endpoint defence.

Detection | Visibility and Rapid Response

Early detection enables faster containment. Monitoring tools within environments such as Microsoft 365 should flag anomalies and unexpected file transfers, new email rules, or unusual login patterns. All of which can signal compromise. Rapid detection is the difference between disruption and disaster.

Education | People Remain the Weakest Link

Most breaches start with human error. Whether through haste, distraction, or misplaced trust, people are the easiest point of entry for attackers. Regular training, phishing simulations, and awareness campaigns reinforce vigilance and build a security-conscious culture across the organisation.

Investing in Modern Security Tools

From zero-trust frameworks and password vaults to dark-web monitoring and shadow-IT detection, cybersecurity tools are now part of every organisation's operational cost base. The key is aligning your investment level with your organisation's risk appetite and regulatory obligations.

Cyber-Insurance: Still Worth It?

Cyber-insurance remains valuable, but only if your organisation meets the insurer's security baseline. Providers increasingly require evidence of robust controls before granting or renewing cover. If your IT team or partner cannot demonstrate compliance, your claim may not be honoured. At Kinetics, we view cyber-insurance as an essential safeguard, but one that must sit on top of strong governance and technical resilience.

Where Do You Start?

Three Steps to Stronger Protection:

01 Policy & Posture (Governance)

Establish clear policies, frameworks, and governance structures for cybersecurity.

Key actions:

- Adopt a recognised framework (CIS, SMB1001, or NIST).
- Develop policies for access, data handling, passwords, and remote work.
- Conduct regular risk assessments.
- Create documented incident response procedures.

→ **Kinetics offers a Policy, Process & Risk — IT Posture Security Review.**

02 People Protection

Employees are both your greatest risk and your strongest defence.

Key actions:

- Monitor user behaviour for anomalies.
- Restrict access to sensitive data.
- Enforce multi-factor authentication and secure password management.
- Provide regular awareness training.

→ **Kinetics offers an Awareness & Practices — IT People Security Review.**

03 Platform Resilience

Ensure systems and applications can withstand and recover from attacks.

Key actions:

- Deploy and maintain firewalls, IDS/IPS, and anti-malware solutions.

- Conduct vulnerability scans and penetration tests regularly.
- Keep systems patched and updated.
- Test backup and recovery plans.

Kinetics offers a Platform — IT Cyber-Vulnerability Security Review.

Essential Cybersecurity Policy Checklist

Use our checklist that summarises essential cybersecurity policies that modern businesses should consider:

Incident Response Policy

In the event of a cybersecurity incident, there is a documented process including reporting procedures, containment and mitigation, investigation, and recovery.

Third-Party Security Policy

Establish guidelines for managing third-party vendors and partners who have access to company resources, including due diligence, contract requirements, and security assessments.

Mobile Device Management (MDM) Policy

Confirmed procedures are in place for managing company-owned mobile devices, including device registration, remote wiping, and software updates.

Access Control Policy

Established guidelines for controlling access to sensitive data and systems, including user account management, password policies, and multifactor authentication.

Data Backup and Recovery Policy

All critical data is backed up regularly, stored securely, and can be recovered quickly in case of data loss or corruption. How far back do your backups go, how frequent are they, and when did you last test them?

Security Awareness Training Policy

Guidelines are in place for educating employees on cybersecurity risks, best practices, and company policies, including periodic training and testing.

Network Security Policy

Guidelines and expectations are current for securing the company's network infrastructure, including firewall configuration, intrusion detection and prevention systems, and access control lists.

Compliance Framework Adoption

Has your organisation adopted a recognised cybersecurity framework such as CIS Controls or SMB1001 to guide your security program?

Conclusion

Cyber threats are now a permanent feature of the business landscape. No organisation is immune, but every organisation can take reasonable, structured steps to reduce its exposure.

Your next actions:

 → Review your cyber-insurance requirements.

 → Ensure current protections exceed last year's baseline.

 → Adopt a recognised framework such as CIS Controls or SMB1001.

Kinetics' managed security solutions — **KARE Foundation** and **KARE Security Plus** — provide ongoing assurance and expert oversight.

It is far better to invest in prevention today than to pay the price of inaction tomorrow.

Strengthen Your Cyber Resilience Today!

 info@kinetics.co.nz

 kinetics.co.nz

 **+64 9 571 1115** **+64 3 974 3139**

 **Auckland Office**
1B, 3 Melrose Street,
Newmarket

Christchurch Office
1/11 Leslie Hills Drive,
Riccarton