November 2025

Strengthening cybersecurity
Key strategies for New Zealand retailers

Employee training and awareness

- **Regular training:** Educate employees on recognising phishing attempts, social engineering tactics, and other cyber threats.
- **Simulated attacks:** Conduct mock phishing campaigns to test and improve employee awareness.
- **Clear policies:** Establish and communicate cybersecurity policies, including acceptable use of company systems and data.

Implement advanced security technologies

- **Multi-Factor Authentication (MFA):** Require MFA for all critical systems to add an extra layer of security beyond passwords.
- **Endpoint protection:** Use antivirus and anti-malware software to protect devices from malicious attacks.
- **Firewalls and intrusion detection systems:** Deploy firewalls and monitor network traffic for suspicious activity.
- **Encryption:** Encrypt sensitive customer and business data, both in transit and at rest.

Regular vulnerability assessments

- **Vulnerability scanning:** Continuously scan systems for weaknesses that could be exploited by attackers.
- **Penetration testing:** Conduct ethical hacking exercises to identify and address vulnerabilities from an attacker's perspective.
- **Patch management:** Regularly update software and systems to fix known vulnerabilities.

Strengthen access controls

- **Role-based access:** Limit access to sensitive data and systems based on job roles and responsibilities.
- **Least privilege principle:** Ensure employees only have access to the information necessary for their tasks.
- **Account monitoring:** Regularly review and deactivate unused accounts, especially for former employees.

Develop a robust incident response plan

- **Preparation:** Create a detailed plan outlining steps to take in the event of a cyber attack.
- **Testing:** Regularly test the plan through simulations to ensure readiness.
- **Communication:** Include strategies for communicating with customers, stakeholders, and regulators during an incident.

Secure third-party relationships

- **Vendor risk management:** Assess the cybersecurity practices of third-party vendors and partners.
- **Contracts:** Include cybersecurity requirements in contracts with suppliers and service providers.
- **Monitoring:** Continuously monitor third-party access to your systems and data.

Invest in cyber insurance

- **Coverage:** Obtain cyber insurance to mitigate financial losses from data breaches, ransomware attacks, and business interruptions.
- **Risk assessment:** Work with insurers to identify vulnerabilities and improve your cybersecurity posture.

Monitor and respond to threats

- **Threat intelligence:** Stay informed about emerging cyber threats and trends in the retail sector.
- **24/7 monitoring:** Use Security Operations Centres (SOCs) or Managed Security Service Providers (MSSPs) to monitor systems around the clock.
- **Incident detection:** Implement tools to detect and respond to threats in real time.

Secure eCommerce platforms

- **Web Application Firewalls (WAFs):** Protect online stores from attacks like SQL injection and cross-site scripting.
- **Secure payment gateways:** Use PCI DSS-compliant payment systems to safeguard customer payment information.
- **Bot protection:** Implement measures to prevent automated attacks, such as credential stuffing or fake account creation.

Comply with regulatory requirements

- **Privacy laws:** Adhere to data protection regulations such as New Zealand's Privacy Act 2020.
- **Audits:** Conduct regular audits to ensure compliance with cybersecurity standards and best practices.
- **Incident reporting:** Be prepared to report breaches to regulators and affected parties as required by law.

Build a culture of cybersecurity

- **Leadership commitment:** Ensure senior management prioritises cybersecurity as a business-critical issue.
- **Cross-department collaboration:** Involve all departments, including IT, HR, and legal, in cybersecurity efforts.
- **Continuous improvement:** Regularly review and update cybersecurity measures to adapt to evolving threats.

About Gallagher

At Gallagher, we've been helping to protect what's important to people and businesses for nearly 50 years. Gallagher is one of the world's top three insurance brokerage and risk management companies, with a network that provides services in more than 130 countries.

Previously known as Crombie Lockwood in New Zealand, we have a long history of helping New Zealanders with their insurance needs.

Connect with us

0800 276 624 | AJG.co.nz

Gallagher INSURANCE