November 2025

Retailers face growing cyber threats in New Zealand

Retailers in New Zealand are facing a growing number of cyber threats, especially targeting their IT systems and email platforms.

As essential components of business operations, these systems can serve as potential gateways for cybercriminals aiming to access and misuse customer information. Understanding these risks and adopting strong security measures is vital for safeguarding business reputation and preserving customer confidence.

Globally, cyber attackers have managed to **cripple some of the largest retail businesses**, and New Zealand is not immune to these threats. While international examples such as Marks & Spencer (M&S) and the Co-op Food chain in the United Kingdom highlight vulnerabilities, New Zealand retailers face similar risks as was experienced early this year by **James Pascoe Group (JPG)**, the parent company behind Farmers, Whitcoulls, Pascoes Jewellers, and Stewart Dawsons. JPG suffered a cyberattack which caused their IT systems to go down, affecting their customer service email channels and store telephone lines, forcing stores across the country to go cash-only.

The consequences of such attacks can be severe. They can result in operational disruptions, revenue losses, and reputational damage. For instance, ransomware attacks can encrypt company servers, locking businesses out of their systems and exposing sensitive customer data. In New Zealand, the retail sector's reliance on digital platforms and customer data makes it a prime target for such attacks.

Cyber threats to New Zealand retailers

Constantly rated within the top five targeted industries[1], New Zealand's retail sector is being increasingly targeted by cybercriminals due to its growing reliance on eCommerce platforms, large volumes of customer data, and interconnected supply chains.

Recent incidents in New Zealand highlight the cyber risks retailers face. Threats targeting:

Third-party vulnerabilities

Retailers relying on external vendors or IT service providers who are at risk of supply chain attacks.

Ransomware attacks

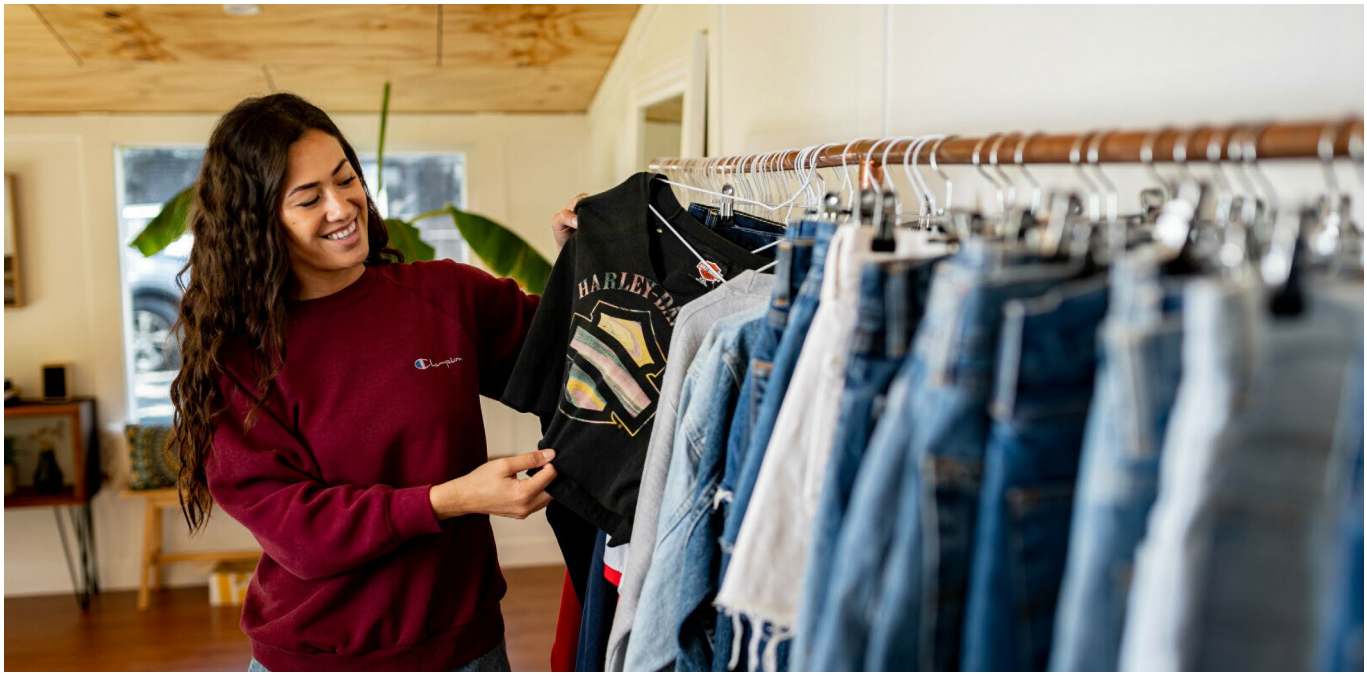
These attacks can disrupt operations and expose sensitive customer information.

Data breaches

The exposure of customer records can lead to regulatory scrutiny and reputational damage.

The regulatory environment in New Zealand is also evolving, with increased scrutiny following high-profile breaches in other sectors. Retailers must now navigate stricter compliance requirements and demonstrate robust cybersecurity measures.

A common misconception is that by outsourcing your IT needs to a third party, you eliminate your risk exposure. If a third party responsible for storing your data experiences a breach, you will likely still bear the responsibility of notifying affected individuals and addressing any resulting regulatory actions.



1 Retail Cybersecurity in 2025: Trends, Risks, and Solutions - Shopify New Zealand

Cyber insurance

Cyber insurance plays a critical role in mitigating financial losses by providing retailers with financial protection and support in the aftermath of a cyber incident. This insurance can also be extended to cover you for data and systems hosted by third parties, as well as business interruption losses stemming from outages at third-party IT providers.

It is now easier than ever to get a quote for cyber insurance without the need to provide complicated technical information. Some insurers now only require basic details such as a company name, website, revenue and employee numbers to provide premium indications.

Here's how cyber insurance can help in the event of a cyber incident

Covers costs of incident response

- **Forensic investigation:** Cyber insurance often covers the cost of hiring cybersecurity experts to investigate the breach, identify vulnerabilities, and determine the extent of the damage.
- **Legal expenses:** It provides coverage for legal fees associated with regulatory compliance, breach notifications, and potential lawsuits.
- **Public Relations (PR) support:** Policies may include PR services to manage reputational damage and restore customer trust.

Compensates for business interruption

- **Revenue loss:** If a cyber attack disrupts operations (e.g. ransomware or denial-of-service attacks), cyber insurance can compensate for lost income during the downtime.
- **Extra expenses:** It may cover additional costs incurred to restore operations, such as renting temporary equipment or hiring external IT support.

Covers data breach costs

- **Notification costs:** Cyber insurance can cover the expenses of notifying affected customers, employees, or stakeholders about a data breach, as required by law.
- **Credit monitoring:** It may pay for credit monitoring services for affected individuals to protect them from identity theft.
- **Data recovery:** Policies often include coverage for restoring or recovering lost or corrupted data.

Provides ransomware and extortion coverage

- **Ransom payments:** Some policies cover the cost of paying a ransom to cybercriminals (though this is subject to legal and ethical considerations).
- **Negotiation services:** Insurers may provide access to experts who can negotiate with attackers to minimise the ransom amount or resolve the situation.

Covers liability and legal claims

- **Third-Party liability:** If a cyber attack results in the exposure of customer or partner data, the policy can cover legal claims and settlements.
- **Regulatory fines:** Some policies may cover fines or penalties imposed by regulators for non-compliance with data protection laws (though this depends on the jurisdiction and policy terms).

Supports IT system restoration

- **System repairs:** Cyber insurance can cover the cost of repairing or replacing damaged IT systems, software, and hardware.
- **Upgrades:** In some cases, policies may contribute to upgrading systems to prevent future attacks.

Example: how cyber insurance works in practice

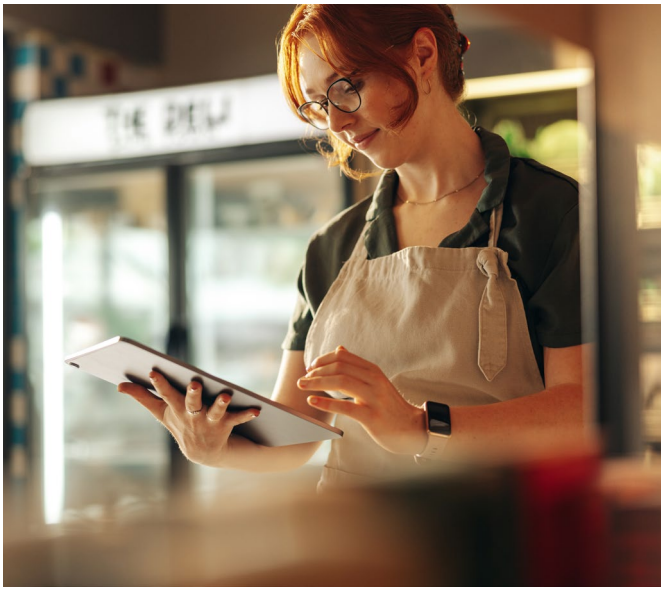
A local online retailer suffered a ransomware attack during their peak holiday sales period, which accounted for over half of their annual revenue. The attack, discovered on Christmas Day, disrupted the retailer's website, CRM, and stock systems.

After activating their cyber policy, a cyber breach coach was appointed that coordinated the various vendors required to assist, including:

- digital forensics experts to contain the breach, restore clean backups and secure systems
- legal services to advise on regulatory requirements; and
- forensic accountants to assist in establishing their business interruption losses.

A few days later operations resumed, although some data recovery continued as investigations revealed staff and customer data had been stolen. As a result, the retailer was advised to notify affected staff and the Office of the Privacy Commissioner under the Privacy Act 2020, with the notifications created by the legal support services provided through their insurance.

The retailer's cyber insurance covered the cost in responding and reimbursed lost profits during downtime. Thanks to the policy's ability to provide swift support, this helped the retailer recover quickly, minimise financial losses, and meet privacy obligations effectively.



Gallagher cyber solutions

Gallagher provides comprehensive support for cyber insurance placement and claims management by leveraging our deep industry expertise, strong insurer relationships, and a client-focused approach, which ensures that retailers are well-equipped to manage their cyber risks and secure the right insurance coverage.

Connect with us to explore how we can support your business in navigating the evolving cyber threat landscape.

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