Cyber Claims: New Zealand Examples

Cyber-attacks are happening here in New Zealand, affecting businesses of all sizes. Insurers are paying real claims, but only where organizations have taken time to arrange Cyber insurance (data deprivation and privacy breach losses) and Crime insurance (funds transfer losses). Some examples of the types of cyber events happening in NZ, and their financial impacts include:

A trading website suffered a denial of service attack when malicious email traffic flooded the site causing it to lock and freeze, denying customers access. The company implemented measures to monitor and track the attacks, and put in place controls to mitigate or negate the impact of them.
A loss adjuster was appointed who worked with the company to assess the claim for significant loss of profits and other remedial costs.
Claim paid: approx $450,000

A service based company was reliant on technology to process and track progress of jobs, that was used as the interface between them and their providers. They were affected by a ransomware attack. External IT forensic costs were incurred for investigation, cleaning and recreating lost data and software from back-up data, including a business interruption claim for extra expenses incurred to manually track progress of jobs. This included an element of loss of profit, as the time excess was exceeded.
Claim paid: approx $130,000

A manufacturing company was affected by a ransomware attack which targeted computers running a certain programme. They encrypted data and demanded a ransom payment in cryptocurrency. External forensic IT costs were incurred for investigation, cleaning and recreating lost data and software from back-up.
Claim paid: approx $100,000

An engineering firm noticed they were unable to access their computer files. Shortly after, an alert was received informing them that their online files had been encrypted by a Cryptolocker virus and payment of a ransom was required to remove encryption. External forensic IT costs were incurred to enable file restoration and to assist that normal business activities were to resume. No ransom was paid.
Claim paid: approx $20,000

An online vendor was notified by its hosting provider that their website had been compromised.
The insurers appointed an IT specialist who was able to mitigate the damage by suspending the site, redirecting traffic to a safe partner site and recommending better practices for the future.
Claim paid: approx $16,000

A large financial advisory practice was left unable to operate when a virus compromised thousands of highly important files. The company provided staff with their work stations and the server however staff worked from their own personal laptops. It was found the employee owned equipment had inconsistent levels of security, and the source was deemed to be an infected email accessed by an unsecured laptop.
Claim paid: approx $13,000

A company was notified by its web-hosting provider that their website had been hacked and was being used to send spam emails.
They suspended the site and instructed the insured to contact a web developer to clean the site.
Claim paid: approx $10,000