What became of the claim?

Cyber Liability Insurance

Event
Just before the year-end holidays, a boutique travel agency was hit by a ransomware attack while senior executives were overseas. The attacker exploited weak password controls and the absence of multi-factor authentication to access the company's systems. They claimed to have stolen over 10 GB of sensitive customer data, including passport details and travel arrangements, and threatened to release it unless a ransom was paid.

Impact
The exposure of personal data created immediate legal and regulatory risks. Delays in notifying both the insurer and affected individuals raised concerns around compliance with privacy laws. Operationally, it disrupted the business during a peak period and triggered internal conflict over whether to negotiate with or pay the attacker.

Data Breach Incident

Response
Delta engaged forensic specialists to investigate the breach, confirm the legitimacy of the threat, and provide guidance on containment and recovery. Legal counsel supported the business in preparing a formal notification to the Privacy Commissioner. Customer support and monitoring were set up to manage concerns of affected parties. Communications experts prepared messages for customers and media aligned with regulatory expectations. Although the company initially considered paying the ransom, Delta advised against it, highlighting that payment would not guarantee the deletion and return of stolen data.

Outcome
The forensic investigation confirmed the breach and provided a clear path to remediation. The Privacy Commissioner reviewed the findings and closed the investigation. Customers and regulators were notified in line with legal obligations. The claim was resolved within five months, and no ransom was paid.

Even with cyber insurance in place, weak security practices can expose a business to significant risk. Delayed reporting can worsen the impact and raise legal concerns. Engaging with threat actors or paying ransoms introduces additional risks with no assurance of a positive result. Stronger security controls are essential, including enforcing MFA, moving away from unsupported/end-of-life systems, training IT teams on breach protocols, and ensuring direct engagement with threat actors is not advised. Regular cyber hygiene audits, phishing simulations, and system vulnerability checks should be part of ongoing risk management. This incident exposed clear gaps in the company's cybersecurity governance.

The claim was managed under Delta's cyber liability insurance policy. The policy provided access to forensic experts, legal and regulatory support, breach response coordination, and public relations services. These resources were critical in handling the incident successfully. ***Learn more here.***

This case study has been modified to de-identify any real-life individuals, events, or organisations (October, 2025).

delta