Steel Pacific
INSURANCE BROKERS

Cyber Insurance in Action

The below information has been supplied by the listed insurers and does not represent claims from entities within the Aviso Group, for more information head to the URLs listed below.

emergence

EXAMPLE	CLAIM SCENARIO	INSURANCE RESPONSE
Cyber Extortion (Ransomware)	The insured experienced unexplained server failures. An ACSC alert confirmed ransomware activity, and investigations revealed persistent unauthorised access, data theft, and exploitation of vulnerabilities over several months. Multiple agencies requested information.	Incident Response experts were engaged immediately. Forensics investigated the cause and secured the systems. Legal counsel managed reporting and notification requirements. Crisis communications specialists handled media and stakeholder queries. Identity support was provided to impacted individuals. **Covered under Section C – Cyber Event Response Costs.**
Business Email Compromise (BEC)	A Microsoft 365 account was hacked, leading to phishing emails being sent to 2,767 recipients. The attacker accessed SharePoint files, including login credentials, and tricked two clients into sending payments to fraudulent accounts.	Legal advice was provided on reporting obligations. Forensics and response services were covered under Section C. The optional **Criminal Financial Loss** cover reimbursed the redirected client payments. The Incident Response team also advised implementing a two-step payment approval process.
Socially Engineered Theft	A staff member received a fraudulent email, appearing to be from a client, with “updated” bank details. Without verification, a significant payment was made to a fraudulent account.	The Incident Response team advised reporting to the bank and checking for further compromise. Despite recovery efforts, funds were lost. The insured was reimbursed under the optional **Criminal Financial Loss** cover, as the electronic transfer constituted a direct financial loss.

Steel Pacific
INSURANCE BROKERS

Business Email Compromise – Medical Practice (1)	A reception mailbox was breached, and phishing emails with malicious links were sent to 1,000+ contacts. Patients expressed concern about their medical data being compromised.	Forensics confirmed the compromise was limited to the reception mailbox and no medical records were impacted. Costs for the investigation were covered under Section C. Communications were drafted to reassure patients.
Cyber Extortion (Ransomware) – Medical Practice (2)	A user reported login issues; the MSP discovered a ransom note. Data was encrypted and exfiltrated from the practice's management software containing sensitive personal information.	Forensics secured the system and investigated the cause. Crisis communications specialists managed media and staff messaging. Ransom negotiators reduced the ransom demand, ensuring compliance with sanctions. **All costs covered under Section C.**
Business Email Compromise – Medical Practice (3)	A compromised email account was used to send phishing emails. The account also contained patient records, reports, Medicare and payment details.	Forensics uncovered a malicious third-party application capable of copying entire mailboxes. Legal counsel provided privacy advice, drafted regulator and patient notifications, and conducted eDiscovery. IDCARE supported affected individuals.

Source: https://emergenceinsurance.com/resources/?_sft_category=claim-examples

DUAL

EXAMPLE	CLAIM SCENARIO	INSURANCE RESPONSE
Property Developer – $19m turnover	Fraudulent correspondence led to a $400,000 payment being redirected overseas.	Optional Social Engineering cover applied. Forensics confirmed the consultant's system was hacked. **Payment: $250,000 (policy sub-limit).**
Not-for-Profit – $9.2m turnover	Supplier's system breach led to donor data being lost.	Legal firm advised on privacy obligations. Notification to the Commissioner was not required. **Payment: $5,900 (legal costs).**
Medical Services – $3.2m turnover	Ransomware locked confidential medical records, halting operations.	Policy triggered for forensics, legal support, and business interruption. **Payment: $63,000.**
Real Estate Agency – $33m turnover	A hacker accessed emails and redirected $3m in payments. $2.8m was recovered, but $200,000 was lost.	Optional **Social Engineering** cover reimbursed losses and covered forensics/legal costs. **Payment: $230,000.**

Steel Pacific
INSURANCE BROKERS

Hairdresser – $3m turnover	A VoIP system was hacked, generating $30,000 in premium-rate calls.	**Social Engineering** cover reimbursed the direct financial loss. **Payment: $30,000.**
Hotel Chain – $1m turnover	Fraudulent email led to a $13,000 payment to a fake contractor account.	Covered under **Social Engineering Fraud** cover. **Payment: $13,000.**
Hotel Chain – $1m turnover	Hacker impersonated a client and redirected $41,000 in payments.	Optional Social Engineering cover reimbursed the financial loss. **Payment: $41,000.**
Accountant – $2m turnover	Hacker accessed systems for two months, compromising 800 client files.	Forensics, monitoring, and legal support (including notification drafting) were provided. **Payment: $90,000.**
Retailer – $5m turnover	Paid $27,000 to a fraudulent supplier. No social engineering cover.	Forensics, monitoring, and legal support (including notification drafting) were provided. **Payment: $90,000.**

CHUBB®

EXAMPLE	CLAIM SCENARIO	INSURANCE RESPONSE
Restaurant /Hospitality	Phishing email installed malware, compromising 400,000 credit card numbers.	Forensics and PCI assessments engaged. **Estimated costs: $1m+ covered.**
Financial Services	Targeted Ryuk ransomware attack with $100k ransom demand. Systems encrypted; backups uncertain.	Incident response coach and forensics retained. First-party expenses ongoing.
Retail	Ransomware shut down servers, registers, online store, and website.	Forensics and response coach engaged. **Mitigation: $1m+;** **Business interruption: $100k.**
Healthcare	Impersonation of a doctor allowed unauthorised access to medical files.	Notifications to patients required. Third-party claims lodged for privacy breaches.

Source: https://www.chubb.com/us-en/business-insurance/products/cyber-insurance/cyber-insurance-claims-scenarios.html

Steel Pacific
INSURANCE BROKERS

LAUW
London Australia Underwriting

EXAMPLE	CLAIM SCENARIO	INSURANCE RESPONSE
Retail	Promotional email accidentally attached a spreadsheet with customer data, including credit card details.	Notification, credit monitoring, and legal costs covered. **Notification/monitoring: $150k; Legal/settlements: $250k.**
Health Clinic	Unauthorised party encrypted medical records and demanded ransom.	Law enforcement involved; $2,500 ransom paid. Business interruption and forensic costs also covered. **Business interruption: $65k; Forensics: $5k.**

Source: 2020-08-10-LAUW-Cyber-Claim-Examples PDF (www.lauw.com.au)

Recovering from a cyber incident without the right insurance can be costly, both financially and reputationally.

Let us help you **find a policy that suits your business needs.**

steelpacific.com.au

ABN: 47 075 780 353 AFSL: 230634