Chubb Cyber Enterprise Risk Management

Loss Scenarios

CHUBB®

Consider the following loss scenarios based on actual claims and then ask yourself whether yo u have adequate insurance in place.

Employee Breaches Internal Governance

Cause of action:
Negligence, Procedure Breach leading to Business Interruption

Coverage triggers:
Business Interruption, Data Asset Loss, Recovery Costs, Incident Response Expenses

Type of organisation:
Retail Store

Number of employees:
20

Annual revenue:
$5 million

Description of event:
An employee at a hardware store ignored internal policies and procedures and opened a seemingly innocuous file attached to an email. The next day the hardware store's stock order and cash registers started to malfunction and business trade was impaired as a result of the network failing.

Resolution:
The hardware store incurred over $100,000 in forensic investigation and restoration services. They also had additional increased working costs of $20,000 and business income loss estimated at $50,000 from the impaired operations.

Total costs associated with the event:
$170,000

Laptop Stolen Results In Invasion of Privacy

Cause of action:
Negligence, stolen laptop leading to an Invasion of Privacy

Coverage triggers:
Incident Response Expenses, Data Asset Loss, Privacy Liability, Business Interruption, Recovery Costs, Regulatory Fines, Potential Payment Card Loss

Type of organisation:
Energy Firm

Number of employees:
100

Annual revenue:
$20 million

Description of event:
An energy company executive's laptop was stolen from a corporate vehicle. The laptop contained significant private customer and employee information. Although the file was encrypted, the overall password protection on the laptop was weak and the PIN for accessing the encrypted information was compromised.

Resolution:
After assessing the nature of the information on the laptop with a forensic expert and outside compliance counsel at a cost of $50,000, the energy company voluntarily notified relevant customers and employees and afforded call centre, monitoring, and restoration services, as appropriate. While the additional first-party cost was $100,000, the energy company also incurred $75,000 in expenses responding to a multi-state regulatory investigation. Ultimately, the company was fined $100,000 for deviating from its publicly stated privacy policy.

Total costs associated with the event:
$325,000

Data Theft Results in Extortion, Business Interruption and Extra Expense

Cause of action:
Breach of Contract and Negligence

Coverage triggers:
Cyber Extortion, Incident Response Expenses, Data Asset Loss, Privacy Liability, Business Interruption, Recovery Costs

Type of organisation:
Solicitor

Number of employees:
55

Annual revenue:
$20 million

Description of event:
An unknown organisation hacked a law firm's network and may have gained access to sensitive client information, including a public company's acquisition target, another public company's prospective patent technology, the draft prospectus of a venture capital client, and a significant number of class-action lists containing plaintiffs' personally identifiable information (PII). A forensic technician hired by the law firm determined that malware had been planted in its network. Soon after, the firm received a call from the intruder seeking $10 million to not place the stolen information online.

Resolution:
The law firm incurred $2 million in expenses associated with a forensic investigation, extortion-related negotiations, a ransom payment, notification, credit and identity monitoring, restoration services and independent counsel fees. It also sustained more than $600,000 in lost business income and extra expenses associated with the system shutdown.

Total costs associated with the event:
$2.6 million

Employee Accesses HR Site, Sells Personal Information

Cause of action:
Negligence and Invasion of Privacy

Coverage triggers:
Incident Response Expenses and Data Asset Loss

Type of organisation:
Professional Services Firm

Number of employees:
25

Annual revenue:
$7.5 million

Description of event:
A rogue employee accessed the human resource platform of a professional service provider. The employee acquired and sold social security information on the black market before being apprehended by law enforcement. Thereafter, several cases of identity theft were perpetrated against the professional service provider's employees.

Resolution:
The professional service provider engaged a forensics investigator and outside compliance counsel. It also notified employees of the breach, established a call centre, and provided monitoring and restoration services to impacted employees.

Total costs associated with the event:
$75,000

Manufacturer Pays For Invasion of Privacy By Intermediary Firm

Cause of action:
Intermediary stealing personal information leading to Negligence and Invasion of Privacy

Coverage triggers:
Incident Response Expenses, Data Asset Loss, Privacy Liability

Type of organisation:
Manufacturer

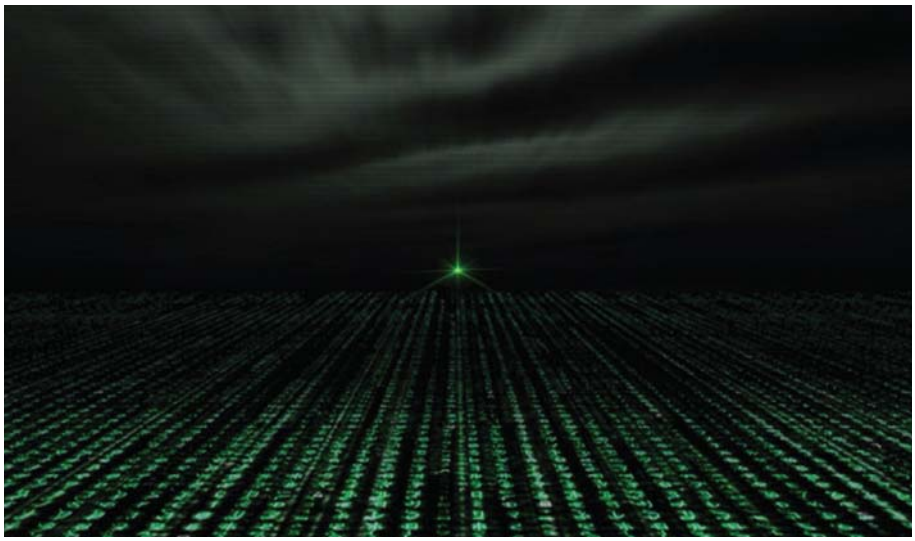
Number of employees:
50

Annual revenue:
$10 million

Description of event:
A manufacturer leased a copy machine over a two-year period. During that period, the company made copies of proprietary client information and its employees' personally identifiable information, including pension account numbers, driver's license numbers and other personal identifiers. After the lease expired, the manufacturer returned the machine to the leasing company through an intermediary company. Prior to making its way back to the leasing company, a rogue employee at the intermediary firm accessed the machine's data for nefarious purposes.

Resolution:
The manufacturer incurred $75,000 in expenses in connection with a forensic investigation, notification, identity monitoring, restoration services and independent counsel fees. It also incurred approximately $100,000 in legal defense.

Total costs associated with the event:
$175,000



About Chubb

Chubb is the world's largest publicly traded property and casualty insurer. Chubb, via acquisitions by its predecessor companies, has been present in Australia for over 50 years. Its operation in Australia (Chubb Insurance Australia Limited) provides specialised and customised coverages include Marine, Property, Liability, Energy, Professional Indemnity, Directors & Officers, Financial Lines, Utilities as well as Accident & Health, for a broad client base, including many of the country's largest companies.

More information can be found at www.chubb.com/au

Contact Us

Chubb Insurance Australia Limited
ABN: 23 001 642 020 AFSL: 239687

Grosvenor Place
Level 38, 225 George Street
Sydney NSW 2000
O +61 2 9335 3200
F +61 2 9335 3411
www.chubb.com/au

Chubb. Insured.℠