# Cyber Claims Examples

## 1.1 SECURITY & PRIVACY LIABILITY

A retailer's marketing strategy included emailing promotions to clients. The insured intended to attach a copy of a flyer detailing a promotion but instead attached a spreadsheet that contained a list of customer names, addresses and credit card information.

Lawyers advised the retailer to notify all affected customers and offered credit monitoring support. All costs incurred in the provision of this service were covered under the **Customer Support and Reputational Expenses** section of the policy.

Several of the affected individuals brought civil proceedings against the retailer. Furthermore, cover for legal costs and indemnification were provided under the **Security and Privacy Liability**. Customer notification and credit monitoring costs were $150,000 and legal fees and settlements made totalled $250,000.

## 1.2 PRIVACY REGULATORY DEFENCE & PENALTIES

A healthcare provider misplaced multiple storage devices which contained sensitive information for over one million patients. The provider could not determine whether the devices were lost, stolen or destroyed. Lawyers advised the company to notify the affected individuals and assisted the company to address a regulatory investigation into the incident which saw the company fined for failing to adequately protect the information.

Cover under this section allowed for the payment of legal fees incurred by the company in connection with responding to the investigation. It also provided coverage for a $75,000 fine. Legal costs were covered and totalled just over $1 million including costs incurred in defending claims brought by affected individuals, costs associated with regulator enquiries, and for miscellaneous notification related work. This type of breach triggers multiple insuring agreements, and overall costs were $2,000,000.

## 1.3 MULTIMEDIA LIABILITY

A financial services company started a blog to convey information to clients and the public. The blog contained a logo/image that was similar to a design that had been copyrighted by another entity.

That entity sent a cease & desist letter to the insured demanding that the insured remove the image from the blog. Discussions between the parties failed to reach a mutually satisfactory result and civil proceedings commenced.

Coverage is available for breach of copyright under the **Multimedia Insuring Clause**. The plaintiff has demanded in excess of $1 million in damages. Legal defence costs (including fees paid to copyright experts) incurred were $250k and a settlement sum of $500k was paid.

## 1.4 DATA RECOVERY & LOSS OF BUSINESS INCOME

A law firm received a cyber extortion threat and ransomware attack on their computer network. All servers (10) were encrypted and these systems provided core business functionality. Unfortunately, the only copy of the backups, those being conducted over the network were also encrypted. Given there was no known way to decrypt this variant of Ransomware, brute-force or otherwise, a decision was made by Underwriters for payment of the ransom of 0.6 Bitcoin (approximately AUD5,300.00).

After a lengthy delay it was confirmed that the decryption key did not work. The insured's IT consultants in the meantime continued a manual rebuild of the insured's computer network focusing on restoring basic function as a matter of priority.

A claim for **first party costs and expenses** and **loss of business income** incurred as a result of a **first party insured event** which occurred on the insured's computer network.

## 1.5 CUSTOMER SUPPORT & REPUTATIONAL EXPENSES

A real estate company discovered malicious software had been uploaded to its servers by an unidentified third party which resulted in corrupted files. Files containing personal information including credit card information had been accessed. Subsequent to the data breach, fraudulent charges were made on various credit cards in multiple countries.

Lawyers advised the company to notify all affected individuals. As a result of the fraudulent credit card transactions, the company offered affected individuals credit monitoring services. These expenses were covered under the **Customer Support and Reputational Expenses** section of the insurance policy. The company also wanted to manage reputational repercussions due to the breach and employed a public relations expert. The fees for the public relations consultant were covered under **Crisis Management Costs**.

The breach resulted in IT forensic investigation fees of approximately $250,000. Other expenses covered by the insurance policy included the cost of identifying and notifying affected individuals, setting up and staffing a call centre to respond to enquiries. Additionally, $150,000 was paid in legal fees to determine reporting requirements and respond to regulatory authorities. Approximately $29,000 was spent on data restoration costs and remediation of IT vulnerabilities and business income loss of $250,000 was paid.

## 1.6 DATA EXTORTION

A small health clinic discovered that an unauthorised third party had gained remote access to a server that contained electronic medical records. The third party posted a message on the network stating that the information on the server had been encrypted and could only be accessed with a password that would be supplied if the insured made a "ransom" payment.

The insured contacted law enforcement and working with law enforcement, determined that the payment ($2,500) should be made. The payment constituted cyber extortion monies under the policy. Furthermore, loss of business income amounted to $65,000 and IT forensic costs of $5,000 were paid in accordance with the coverage provided by other sections of the policy.

## 1.7 TELEPHONE PHREAKING

A media company discovered that their phone systems were being used to make unauthorised calls and being charged $5,000 by their telephone service provider.

After forensic investigations, it was discovered that hackers infiltrated their computer network to make these calls.
The total $5,000 was covered in the policy and paid back to the media company.

## 1.8 CYBER CRIME

While on holidays a CEO of manufacturing company's email account was hacked by an unknown third party and impersonating to be the CEO.

The hacker issued instructions to an employee (accountant) to transfer two lots of $50,000 from the company's trust account to a fraudulent bank account.

The first $50,000 transaction went through, however the second transaction was stopped by the bank and the CEO was informed. The CEO confirmed they did not authorise the transaction.

The Bank's fraud team and Australian Federal Police Cybercrime Online Reporting Network (ACORN) were made aware of the incident.
Unfortunately, the first transaction of $50,000 was not recovered and **Cyber Crime** clause was triggered under the policy and funds paid to the company.