CYBER INSURANCE - CLAIMS EXAMPLES

KBI
Specialist Insurance Brokers

SOCIAL ENGINEERING – VENDOR EMAIL HACKED

The controller for a distributor of component parts was responsible for making regular payments to overseas vendors from which the distributor purchased products for resale in the United States. After many months of working with one particular vendor and receiving regular shipments, the controller received an email that appeared to come from his vendor contact, indicating that the vendor's bank was having issues with accepting payments, and asking if the next payment could be made to a new bank. Due to the vendor's overseas location, verification was a challenge. After the supposed vendor applied some pressure, the controller paid the invoice via wire transfer.

The following month, when the real vendor realised that its best customer's payment was overdue, an investigation determined that the vendor's email had been hacked, and an imposter had been socially engineering the company into believing that the change in bank information was authentic. In the end, the fraudster finagled almost $250,000 from the distributor.

** This claims example has been provided by Chubb Insurance Company of Australia Limited **

EMPLOYEE ERROR (FIRST PARTY & THIRD-PARTY CLAIM)

A retailer emailed a group of customers to promote a sale with special discounts available to them. The retailer intended to attach a copy of the flyer detailing the discounts but instead attached a copy of a spreadsheet that contained a customer list, including customer names, addresses and credit card information.
The retailer was required to notify all affected customers of the error and offered credit monitoring services.
Several of the affected individuals began legal proceedings against the retailer. The notification and credit monitoring costs totalled $50,000, and the amount to settle the legal proceedings with the retailer's customers combined with the associated legal costs and expenses totalled $100,000.
Most Cyber Risk Insurance policies provide coverage for breach of privacy which includes legal costs, indemnification of third parties and crisis management costs.

** This claims example has been provided by Insurance Australia Group Limited **

PRIVACY BREACH, FINES & INVESTIGATION (FIRST PARTY & THIRD-PARTY CLAIM)

An IT company misplaced multiple drives that contained personal information for over one million customers. It was unknown whether the drives were lost, stolen or destroyed. The IT company was required to notify the affected individuals, as well as the privacy regulator. The regulator investigated the incident and fined the company for failing to have appropriate safeguards in place to protect customer information.

The company incurred legal fees of $1,000,000 in connection with the regulatory investigation and defending legal actions brought by affected customers and for the costs and expenses in notifying customers their personal information had been lost, stolen or destroyed. The company was also fined $75,000 by the privacy regulator. The total loss to the company exceeded $5,000,000.

This type of scenario triggers multiple Insuring Clauses under a typically Cyber Insurance policy, including privacy fines and investigations.

RANSOMWARE

A professional services company was affected by cryptolocker virus identified as the Lockey virus. A network of 20 computers were affected with users unable to access files, which had been encrypted. Investigations revealed the virus entered the computer network via an infected email attachment which had been inadvertently opened by an employee.

An IT specialist was brought in to re-build and restore lost data from the back-up server. The IT costs involved in containing and recovering from the incident were claimed under the Cyber Insurance policy. No ransom was paid as a result of the data recovery efforts.

DDOS – DISTRIBUTED DENIAL OF SERVICE

An online service provided was hit by a Distributed Denial of Service (DDoS) attack. The DDoS attacks effectively starved the web site host system of resources by flooding it with malicious traffic and preventing legitimate customers logging on or accessing the website. Account Customers utilising the Internet, Mobile Phones and Mobile Apps were unable to log on, new users were unable to set up accounts.

A specialist forensic IT vendor was appointed to investigate and mitigate the attack. The incident involved serious disruption to the insured's business and loss of income as a result of its website being down for approximately one week at one of the busiest times of the year. The Cyber Security Insurance policy responded to the costs of the IT investigation and remediation and the loss of profits suffered.

DATA BREACH

Users of the Insured's online network had reported that they had received spam emails from an individual they knew to be an ex-employee of the Insured, to a unique email address that they had created exclusively for use on the Insured's website. Investigations confirmed that while working for the Insured, the ex-employee had access to the relevant customer databases and forensic IT investigations confirmed the data breach.

Steps were taken to ensure that the ex-employee deleted the data and signed an enforceable undertaking not to use the data in future. The quick action to contain the breach and engage with the regulator meant that the regulatory investigation could be responded to in a way that satisfied the regulator and the costs and risk could be contained.

** These claims examples have been provided by AIG Australia Limited, Chubb Insurance Company of Australia Limited, and Insurance Australia Group Limited **