Cyber Risk and Insurance
Claims Examples

Unauthorised access to network

A legal firm's network was hacked by an unknown source that gained access to sensitive client information including lists containing personally identifiable information (PII). A forensic technician hired by the legal firm determined that malware had been planted in the network. After the hack, the legal firm received a phone call from the hacker seeking a payment of $10m to not place the stolen client information online.

Impact

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

Employee illegally accessed client and employee data

During a 2-year period, a business that leased a copying machine made copies of proprietary client information and employees details including driver's license numbers and other personal identifiers. After the lease expired, an intermediary company collected the machine to return to the leasing company. Prior to the return, a rogue employee accessed the machine's data to use for illegal purposes.

Impact

The business incurred $75,000 in expenses from the forensic investigation, notification, identity monitoring, restoration services and independent counsel fees, along with $100,000 in legal fees.

Identify theft

An employee illegally accessed their employers human resource platform and acquired and subsequently sold some of the staff's personal information. After this illegal access of information, several staff experienced identity theft.

Impact

The impacted business engaged a forensics investigator and legal counsel. It notified all employees of the breach, established a call centre, and provided monitoring and restoration services to the impacted employees. The costs associated with this event totalled $75,000.

Website rendered inaccessible

During a fundraising campaign, a charity's website was targeted with a denial of service attack, crippling the functionality of the site. This made it impossible for people to make online donations during the final days of the fundraising campaign.

Outcome

The charity received a payment of $1.5m for the lost donations due to the attack, and to rectify the damage to the website.