Cyber Liability and Privacy Protection Claims Scenarios

Eye Surgery Clinic

- Two (2) locations
- 15 staff
- $12M turnover

Background

An employee opened an email attachment that contained a virus. Once opened an encrypted virus was spread, causing the Insured to lose access to their network. The Russian hackers demanded ransom payment in BITCOIN of $6,000. Both practises were able to function normally (albeit slowly) in terms of accepting and treating patients by using paper records. However, the business was not able to raise invoices as this is part of a paperless system. Forensic Investigators were able to recover the vast majority of data and restore the paperless system.

Outcome

The policy was triggered and Forensic Investigators were able to recover the vast majority of data and restore the paperless system. $90,000 in IT expenses, First Party damage and lost man hours.

Payment: $90,000

Real Estate Agents

- 6 staff
- $8M turnover

Background

The insured had a Ransomware virus enter their computer system where the hacker demanded a payment of US$500 to be made. The insured's business was unable to function normally for 7 days.

Outcome

The policy was triggered and $7,440 was paid to cover the cost of restoring information, payment, as well as lost man hours.

Payment: $7,440

Family Owned Beverage and Snack Sales and Distribution

- 15 staff
- $2M turnover

Background

A CrytopLocker virus infected the Insured's network forcing them to take their computers offline. It was found that the virus had also encrypted company files. A second virus was then detected, which required the server to be rebooted. This resulted in critical network outage with the sales team unable to send any orders for 2 days.

Outcome

The policy was triggered and $3,470 was paid in IT expenses and lost revenue.

Payment: $3,470

Diesel Service and Repair Agents

- 15 staff
- $4M turnover

Background

An employee of the Insured opened a zip file attachment to an email which deployed a variant of ransomware malware. All the files used to open the attachment were encrypted as well as the Insured's drop box files in the Cloud which included HR files and employee personal data.

Engineers were able to carry on with their operations however all administrative tasks at the Insured's ceased. DUALs breach response team conducted a standard enquiry with the Insured's IT provider into the causation and scope. An investigation was carried out into whether a data compromise occurred given the hackers were able to access files which contained HR and personal data.

Outcome

The policy was triggered and $5,000 was paid for loss of man hours and IT expenses to repair systems.

Payment: $5,000

Engineer

- 20 staff incl 3 admin
- $18M turnover

Background

The Insured had been hit with a Ransomware virus causing the server to become totally encrypted and inoperable. The extortion demand was in BITCOIN and equivalent to $10,000. The Insured decided to pay the ransom because it was discovered that there was no viable back-up of their data to restore. Remote logins were also not possible. Once the ransom had been paid, the Insured was provided with a decryption code which restored their system.

Outcome

The policy was triggered and $18,650 was paid for IT expenses to restore the system from scratch.

Payment: $18,650

Accountant

- 20 staff
- $3.5M turnover

Background

A former IT contractor allegedly logged-in remotely without authorisation and deleted files on the Insured's server. They also embedded spyware and downloaded viruses onto the server. However, when the police interviewed the individual, he advised that all of his computers were stolen before the Insured's computers were hacked.

Outcome

The policy was triggered and $8,000 was paid for costs incurred while restoring and repairing the server damage caused by this incident.

Payment: $8,000

Online Clothing Retailer

- 5 staff
- $2M turnover

Background

On two occasions, in January and March 2017, the Insured's computer system was affected by a CryptoLocker virus which prevented the Insured from being able to operate as usual.

Outcome

The policy was triggered and $14,000 was paid for IT expenses to restore the Insured's systems back to the position they were in before the virus.

Payment: $14,000

Real Estate Agents

- 15 staff
- $10M turnover

Background

The Insured's network was hacked over a long weekend. The Insured deployed their existing IT outsource arrangements to respond to the attack and sought to recover these expenses as well as any additional man hours incurred during the aftermath, to return the business to normal operations.

Outcome

The policy was triggered and $8,680 was paid for the cost of restoring the network and $2,000 in additional staff hours.

Payment: $8,680

Raw Materials Manufacturer

- 28 staff
- $7.5M turnover

Background

The Insured's system was hacked via an email they received carrying a Ransomware virus. The virus prevented them from having any access to emails and their network. The hacker held the clients system to ransom and would only release files if the client's paid $12,500.

The fact that the client had numerous file shares and common storage areas made their system particularly vulnerable to attack and made it easy for the hacker to encrypt nearly every file in their system.

Outcome

The policy was triggered and $12,500 was paid for the ransom plus an additional $25,000 in IT expenses related to diagnosing the problem, decommissioning the old servers and installing a new network.

Payment: $12,500

Catering Company

- 7 staff
- $1M turnover

Background

An email was sent to the Insured's main email address (found on their website) which contained a virus. It resulted in an immediate ransom demand being received and malware virus spreading through their network.

All the Insured's servers were affected and they were unable to use their payroll system for 2 weeks and had to resort to manual processes.

The client's IT provider identified the issue and had to install new software. DUALs breach response team worked with the Insured's IT provider in the remediation plan in response to the attack.

Outcome

The policy was triggered and $15,000 was paid for IT expenses to install new software and lost revenue.

Payment: $15,000

Lumber and Building Materials Wholesaler

- 7 staff
- $1M turnover

Background

The Insured's system was hacked by a CryptoLocker virus which prevented employees from opening files and accessing the public drives. DUALs breach response team investigated the matter and installed new software to prevent another attack.

Outcome

The policy was triggered and $19,000 was paid for IT expenses and lost revenue.

Payment: $19,000

Steel Manufacturer

- 65 staff
- $15M turnover

Background

The Insured's network was infected with a CryptoLocker virus. DUAL's breach response team instructed the client's IT provider to remove all workstations and take servers off the network to cleanse them.

Outcome

The policy was triggered and $10,000 was paid for IT related expenses.

Payment: $10,000

Architect

- 5 staff
- $1.8M turnover

Background

The Insured's network was infected with a virus that was received via email and allowed the hacker to gain access to the Insured's website. DUALs breach response team investigated the matter and removed the virus and reinstated their website.

Outcome

The policy was triggered and $5,100 was paid in IT expenses.

Payment: $5,100

Medical Company

- 6 staff
- $2M turnover

Background

An email opened by an employee caused a virus to infect the system including personal information of patients. DUALs breach response team were notified and shut down the server. Data was recovered from Backup drives and new software was installed.

Outcome

The policy was triggered and $17,000 was paid in IT expenses.

Payment: $17,000

Landscaper

- 3 staff
- $900K turnover

Background

Insured experienced a Malware infection on their computer which required all servers to be restored. DUALs breach response team responded to the attack and cleansed the system.

Outcome

The policy was triggered and $2,000 was paid to reimburse the client for IT expenses.

Payment: $2,000

Insurance Broker

- 2 staff
- $1M turnover

Background

A malicious code was installed on the Insured's website which resulted in them being added to a domain blacklisting site as a company that contained malware. Client engagement was affected as emails were not being received or contained warnings about their content which caused the Insured reputational damage.

Outcome

The policy was triggered and $17,000 was paid in IT expenses and reputational damage. .

Payment: $17,000