Cyber and Data Security Insurance

Cover Summary

This is only a summary of the cover which may be provided under each section of cover. How the policy will respond will depend upon the facts and circumstances of the individual claim. Please see policy wording for full details of coverage.

Cyber, data security and multimedia cover

- Liability arising out of multimedia exposures as a result of a hacker. For example defamation, libel and unintentional infringement of intellectual property rights
- Liability arising from the failure to properly handle, manage, store, destroy or otherwise control personally identifiable information
- Liability arising out of unintentional transmission of a computer virus
- Liability arising out of a hacker's fraudulent use of information
- The costs of any financial benefit that has been transferred to a third party that cannot be recouped and has occurred as a result of a covered loss
- The costs to withdraw or alter data or images or other website content as a result of a court order or to mitigate a claim
- The costs to replace or restore documents discovered by the insured to be lost, damaged or destroyed
- Compensation costs arising as a result of directors, partners and employees attending court in connection with a covered claim
- Defence costs

Data breach notification costs cover

- The provision of consumer notifications to comply with data breach law following a data breach
- The legal fees incurred to identify notification communication obligations and draft notification communications
- The costs to send and administer notification communications
- The costs of call centre services to respond to enquiries and queries following a notification communication

Information and communication asset rectification costs cover

- The costs to repair, restore or replace the affected parts of the insured's information and communication assets after they were damaged, destroyed, altered, corrupted, copied, stolen or misused by a hacker

Regulatory defence and penalty costs cover

- Payment for those amounts which the insured is legally obliged to pay (including legal and defence costs) as a result of a civil regulatory action, regulatory compensatory award, civil penalty, or fines to the extent insurable by law, imposed by a government or public authority regulator

Public relations costs cover

- Payment for all reasonable costs the insured incurs for a public relations and crisis management consultant to avert or mitigate any material damage to any of the insured's brands and business operations

Forensics costs cover

- Payment for a forensic consultant to establish the identity or methods of the hacker or other details required by the insurer following a data breach
- Payment for a security specialist to assess the insured's electronic security and the costs of reasonable security improvement
- Payment for the temporary storage of the insured's electronic data at a third-party host location, if it is viewed that the insured's information and communication assets remain vulnerable to damage, destruction, alteration, corruption, copying, stealing or misuse by a hacker

Credit monitoring costs cover

- Payment for credit monitoring services in order to comply with data breach law

Cyber business interruption cover

- Payment for loss of business income, as a result of the total or partial interruption, degradation in service, or failure of information and communication assets following a failure by the insured or a service provider to protect against unauthorised access to, unauthorised use of, a denial of service attack against, or transmission of a computer virus to, information and communication assets

Cyber extortion cover

- Payment for reasonable and necessary expenses incurred by the insured including the value of any ransom paid by the insured for the purpose of terminating a cyber-extortion threat

What if there is a cyber-attack in my business?

Scenario

Employee 'A' of Company 'X' is unable to access any documents on their work computer. Employee 'A' reports this to their IT department and after a quick investigation it is discovered that the employee's drive is affected by malware.

Company 'X' has large amounts of sensitive personal identifiable information including passport details, customer and employee information, credit card details etc. On investigation of Employee 'A's computer it appears that access has been made to this data using Employee 'A's credentials.

At the same time, a valued customer of Company 'X' receives three telephone messages from an individual claiming to be an employee of Company 'X'.

Client's response

Covered by QBE cyber and data security insurance, Company 'X' immediately takes the following steps:

1. Notifies the QBE data breach response service
2. Changes Employee 'A's password and suspends the employee's account
3. Restores the affected drive from the last back up (five days prior to the incident)

QBE's response

How does QBE's 'Cyber and Data Security' insurance policy respond?

Cyber, data security and multimedia cover

- ✓ Covers for the failure of the insured to protect against unauthorised access to, unauthorised use of, a denial of service attack against, or transmission of a computer virus to information and communication assets

Forensic costs cover

A hired forensic analyst:

- ✓ Locates the source of the malware
- ✓ Analyses the exact nature of the malware and evaluates the business impact
- ✓ Ensures containment and that no further malware is in the system
- ✓ Establishes if a breach has occurred and potential extent of loss

Compensation paid: US$35,000

Other typical scenarios which could have been mitigated by our cyber and data security insurance policy:

The malware damaged Employee A's hard-drive and it now needs replacing:

Information and communication asset rectification costs cover
Costs to repair, restore or replace the affected parts of the information and communication assets to the same equivalent standard, condition, functionality, level of service and/or with the same content.

Data was stolen and more than 3,000 credit card details were compromised:

Data breach notification costs cover
The legal fees incurred to identify notification communication obligations and draft notification communications. The costs to send and administer notification communications. The costs of call centre services to respond to enquiries and queries following a notification communication.

Regulatory defence and penalty costs cover
Cost of civil regulatory actions, civil penalties/fines imposed by Government or privacy authority.

Credit monitoring costs cover
Costs of monitoring credit files to spot potential misuse or identity theft.

The local newspaper is tipped off about the data breach and asks Company 'X' for a statement before printing their story in the next edition:

Public relations costs cover
Costs incurred for a public relations and crisis management consultant to neutralise and mitigate any reputational damage to any of the insured's brands and business operations.

The hacker returns. Threatening to publish the financial data of your customers unless a ransom of US$30,000 is paid:

Cyber extortion cover
Payment for reasonable and necessary expenses incurred by the insured including the value of any ransom paid by the insured for the purpose of terminating a cyber-extortion threat.

A few weeks later another employee of Company 'A' speaks at an industry specific conference and allege that a number of competitors have also been involved in hack-attacks which were handled very poorly:

Cyber, data security and multimedia cover
Any allegations of defamation or infringement of intellectual property rights.

At QBE, we are committed to providing protection and assurance for cyber and data security for your business.

QBE