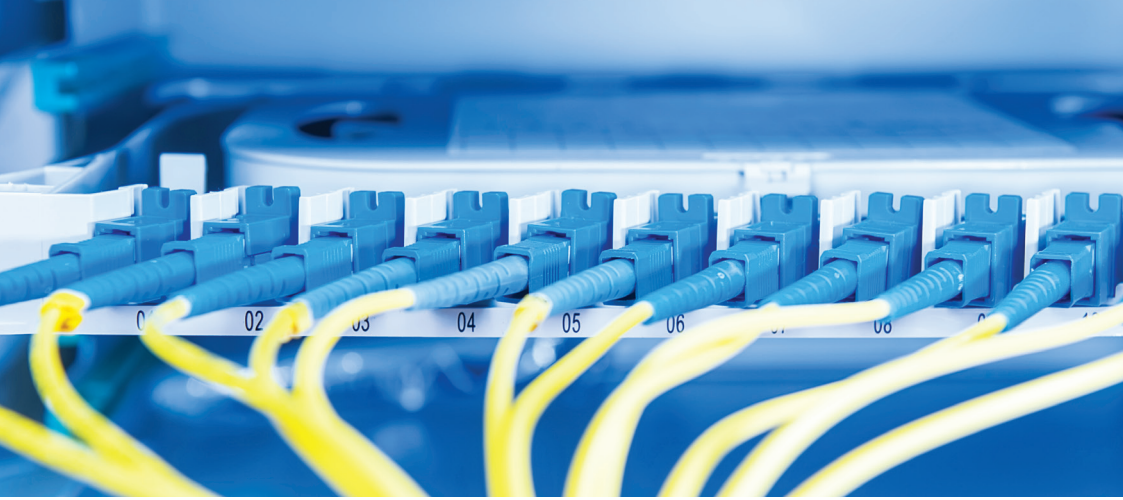
QBE

Cyber and Data Security Insurance



Is my business safe from cyber-attacks?

Unfortunately no business today is safe from cyber-attacks. Even institutions such as multinational banks, government networks and telecommunications providers, which have some of the most advanced cyber defence systems in the world, still fall victim to attacks.

Small and medium-sized businesses often face an even higher risk of cyber-attacks than larger entities simply because they have less robust cyber-attack prevention controls. This risk to SMEs further increases for organisations who trade online and or hold quantities of customer data. If your business has any web presence and has any sensitive or financial data — such as credit details or health records — it can quickly become a target.

Does my existing insurance cover cyber and data security?

- It is best to check to be sure. Some Professional Indemnity policies may include a degree of third party cyber liability cover, but typically do not cover first party cyber risks such as the repair and recovery of computer systems damaged by a hacker.
- Cyber extensions for General Liability, Professional Indemnity or Directors' & Officers' insurance generally provides basic third party cover, but usually do not cover first party risks such as payments for or expenses related to cyber-extortion threats.
- Business interruptions may be covered by your Property policy, however, such does not usually include interruptions caused by non-physical damage — the interruption or failure of your computer systems for example.

For security and assurance, we always recommend that you protect yourself and your business with a standalone cyber and data security insurance policy.

What are the five main cyber-threats to your business?

Often, when we think of cyber and data security, we associate any breach with malicious behaviour or external attack. While such breaches are widespread and on the rise, the loss or breach of data can also be the result of innocent human error or system failure. Any kind of security breach can have detrimental impacts on your business. Below are the five most common threats:

Ransomware and extortion: Usually involves malware infecting your business' network which locks all access to systems, with a ransom message demanding payment.

Financial transfer phishing: Targeting any form of financial transaction between entities, the hacker sends fake communication with incorrect bank details in an attempt to direct the transaction to the hackers account.

Software exposure: One of the scariest threats from an industry standpoint is systemic exposure from attacks on common forms of software used by an entire industry group. For example, if a security loophole is found in a common system, like bookkeeping software, resulting in data from thousands of practices being locked and held ransom by hackers.

Internal threats: Simple human error with no malicious intent, for instance losing a company laptop containing client data could cause significant damage to your business. Malicious attacks by employees are other threats which can have devastating effects on your business.

Data exfiltration: Once a hacker has infected your business with malware, they may decide to be more discrete and try to steal as much confidential data as possible without being detected. Once the data is stolen they either sell off the data or use it to commit various forms of financial fraud.

How can you protect your business?

Effective risk management is fundamental to protect your business. Adequate and up-to-date risk management controls are essential for all businesses and provide considerable protection against malicious and non-malicious activities. However, breaches can still occur and when things go wrong insurance policies provide extra security and protection.

Risk management advice

- Regular strengthening and updating of all business applications;
- Restrict and monitor user privileges to operating systems and applications based on user duties;
- Deploy network security and anti-malware protection software to prevent unauthorised access and malicious content; and
- Establish a cyber incident response and disaster recovery plan, train employees, test and continuously improve all aspects of the risk management framework.

Cyber and Data Security offering

Cover is provided on a first and third party basis. Including:

Third Party Cover:

Cyber, data security and multimedia cover

- Compensation to third parties for the failure to protect their information held by the insured.

First Party Cover:

Data breach notification costs cover

- As a result of a breach of data held by the insured, cover is provided to pay for the expenses incurred or obliged to pay to notify consumers of the breach, legal fees to assist with communications and costs associated with administering the notification process.

Information and communication asset rectification costs cover

- Repair, restoration or replacement of the insured's computer systems where they were damaged, destroyed, altered, corrupted or misused by a hacker.

Regulatory defence and penalty costs cover

- Payment related to a regulatory action, penalty or fine (where insurable by law).

Public relations costs cover

- Payment incurred for a public relations and crisis management consultant to avert or mitigate any damage to the insured's brand or operations.

Forensics costs cover

- Payment for a forensic consultant to identify a hacker, a security specialist to assess electronic security and temporary storage of the insured's electronic data.

Credit monitoring costs cover

- Payment incurred for a credit monitoring service to comply with data breach law.

Cyber business interruption cover

- Reimburse for the loss of business income as a result of the interruption, degradation in service or failure of the insured's computer systems.

Cyber extortion cover

- Payment for the expenses arising from a cyber-extortion threat.

How will you benefit from partnering with QBE?

1. **High claims paying capability:** Our strong balance sheet ensures a sustainable, long-term partner with strong financial ratings. For our latest ratings, please refer to our Group's website (www.group.qbe.com/investor-centre/ratings).

2. **Expert claims handling:** We understand that the true test of any insurance company is when a claim arises. Thus, QBE has local claims representatives and legally qualified claims specialists dedicated to assist through the entire claims process. QBE has direct access to Cyber Incident Managers and Forensic Investigators who specialise in mitigating cyber incidents and will ensure your business swiftly returns to pre-loss operation.

3. **Global reach and remarkable history:** QBE ranks in the top 20 of all global insurers and reinsurers with over 14,000 people in 37 countries. We have been present in Asia Pacific for more than 130 years and now operate in 15 key markets, including a representative office in mainland China.

4. **Broad and transparent coverage:** QBE's cyber and data security wording is broad and easy-to-read with no hidden exclusions so both intermediaries and clients can fully understand the coverage.

5. **Trusted advisor:** QBE is a global insurer with a long track record of assisting our valuable customers. Our specialised cyber and data security underwriters and claims partners are hand-picked for their technical knowledge and commitment to high service levels.

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

QBE Insurance (Singapore) Pte Ltd
A member of the worldwide QBE Insurance Group Unique Entity No. 198401363C

1 Raffles Quay #29-10
South Tower Singapore 048583
Tel : (65) 6224 6633
www.qbe.com.sg