Cyber Liability Insurance

Coverage Overview

1st Party Coverages

Breach Reponses Costs	This covers on-going forensic investigation and credit monitoring costs (up to 2 years) as well as the engagement of a public relations firm to contain the public fall out following a privacy breach.
Crisis Management and Public Relations	Coverage for expenses to mitigate loss due to a public relation event such as costs incurred for a public relations consultant, media purchasing to inform general public about the event, or notifying individuals who are not required to be notified by breach of law.
Ransomware and Cyber Extortion	Money paid on the Insured's behalf in response to a ransomware attack.
Direct and Contingent Business Interruption	Coverage for loss of net profit and additional costs of working following a cyber event and for loss of net profit following a cyber event which impact an external supplier upon which the business relies.
Digital Asset Restoration	Coverage for restoration costs incurred resulting from a security/systems failure.
Reputational Harm Loss	Coverage for the lost net profits resulting from an adverse publication concerning a security failure, data breach, or cyber extortion suffered by a policyholder that affects their customers or clients.

3rd Party Coverages

Network and Information Security Liability	Coverage for claims brought against the insured by a third party following a cyber event. Claims will commonly relate to a loss of third-party data, a security breach resulting in a system denial of access, a privacy breach or a negligent transmission of malware.
Regulatory Defence and Penalties	Coverage for defence costs and regulatory fines and penalties resulting from a security failure or data breach (subject to applicable law).
PCI Fines and Assessment	Coverage for PCI fines or assessments made against a policyholder resulting from a security failure or data breach. The cost of Assessments often far exceeds those of the Fines & Penalties and include the fraudulent purchases that are made using the compromised card details, the costs of reissuing cards and investigating the extent of any misuse of the card data.

Funds Transfer Liability	Coverage for defence costs and damages from liability to a third party for fraudulent transfers of funds owed to another party resulting from a failure in the policyholder’s security.
Multimedia Content Liability	Coverage for defence costs and damages from liability to a third party for multimedia wrongful acts, such as infringement, defamation, or piracy.

Ancillary (non-core) Coverages

Negotiable coverages which are not common place in the market.

Proof of Loss Preparation Expenses	Coverage for a third-party forensic accounting firm to assist with preparing proof of loss required under this policy.
Computer Replacement and Bricking	Coverage for the costs associated with replacing computer hardware whose integrity has been permanently altered by malware.
Court Attendance	Coverage for reasonable costs and expenses when we request policyholders attend a trial, hearing, deposition, mediation, arbitration, or other proceeding relating to the defence of any claim.
Criminal Reward	Coverage for a reward for information that leads to the arrest and conviction of anyone who commits, or tries to commit, an illegal act related to coverage under our policy.
Funds Transfer Fraud, Personal Funds Fraud, and Social Engineering	Coverage for direct financial loss caused by a targeted deception of the insured by a third party resulting in the unrecoverable transfer of funds.
Service Fraud including Cryptojacking	Coverage for direct financial loss as a result of being charged a fee for the fraudulent use of business service.
Impersonation Repair Costs	Coverage for costs to retain a law/public relations firm to publish press release to advise customers of impersonation fraud, costs to reimburse existing clients.
Invoice Manipulation	Coverage for direct net costs (excluding any profit), for which a policyholder is unable to collect payment as the direct result of their customer being tricked into sending the payment to a fraudster.

Several insurers also offer complimentary services to support SME businesses in managing and mitigating cyber risks. Examples include:

- Guidance to develop and tailor an incident response plan (IRP)
- Real-time cyber threat alerts
- Dark web monitoring
- Tabletop incident response exercises (may be subject to an additional premium)