Data and systems are key assets for most companies because without them you cease to exist. iTOO Cyber Insurance provides your business with access to expert knowledge and resources to effectively manage and recover from a cyber incident.

Policy Triggers

01. CYBER EXTORTION

02. DENIAL OF SERVICE

03. MALWARE

04. HACKING

05. INSIDER AND PRIVILEGE MISUSE
Internal and service provider.

06. DOWNSTREAM ATTACK
Your environment resulting in damages to another.

07. PHYSICAL THEFT AND LOSS
Both devices and physical hard copy data.

08. BUSINESS EMAIL COMPROMISES

Our comprehensive cyber insurance policy can be tailored to your requirements and provides the following coverages:

1ST PARTY

Regulatory fines
To the extent insurable by law, fines imposed by a government regulatory body due to an information privacy breach.

Business interruption
Loss of income and increased cost of working because of a systems security incident.

Data restoration
Costs to restore, re-collect or replace data lost, stolen or corrupted due to a systems security incident.

Outsourced service provider
Cover for exposure from named outsourced service providers including business interruption losses.

Theft of Funds
Unrecoverable loss of money, belonging to or for which you are legally responsible, as a direct result of a system security incident by a third party. Cryptocurrency losses are excluded.

Payment card industry fines & penalties
Cover for monetary fines, penalties, assessments, chargebacks, reimbursements and fraud recoveries which you become legally obligated to pay in terms of a merchant services agreement.

Phone phreaking
Call and/or bandwidth usage costs you are legally obligated to pay as a result of unauthorised use of your telecommunications system by a third party.

Physical damage
Costs to replace or repair direct physical damage of tangible property belonging to or rented, leased or hired by you as a direct result of a system security incident.

3RD PARTY

Privacy liability
Defence and settlement of liability claims arising from compromised information.

Network security liability
Defence and settlement of liability claims resulting from a system security incident affecting systems and data as well as causing harm to third-party systems and data.

Media liability
Defense and settlement of liability claims resulting from disseminated content (including social media content) including unintentional defamation or copyright infringement.

INCIDENT RESPONSE

Incident response costs
Costs to respond to a system's security incident, including:

- for professional (legal, public relations and IT forensics) advice, including assistance in managing the incident, coordinating response activities, and making representation to regulatory bodies;
- to perform incident triage and forensic investigations, including IT experts to confirm and determine the cause of the incident, the extent of the damage including data compromised, contain, mitigate, and repair the damage, and guidance on measures to prevent re-occurrence;
- for crisis communications and public relations costs to manage a reputational crisis, including spokesperson training and social media monitoring;
- for communications to notify affected parties; and
- for remediation services such as identity theft monitoring to protect affected parties from suffering further damages.

CYBER EXTORTION

Costs to investigate and mitigate a cyber extortion threat. Where required, 50% of the costs to comply with a cyber extortion demand.