

# CYBER INSURANCE TRIGGERS

## Network breach:

**When someone gets into your computer system or network:**

- Being hacked (unauthorised access or use).
- Data being stolen (like client information or intellectual property).
- Viruses or malware.
- Overloading your system so it crashes (denial of service attack).
- Physical theft of both devices and physical hard copy data.
- Causing harm to others by attacking them through system (called a downstream attack).

## Privacy breach:

**This happens when private or confidential information is:**

- Leaked
- Exposed
- Misused

and can involve personal data of employees, customers, contractors, suppliers or anyone else.

## Incident mitigation

**Incident response costs**

Costs to respond to the incident, including:

- Perform incident triage and forensic investigations, including IT experts to confirm and determine the cause of the incident, the extent of the damage including the nature and volume of data compromised, how to contain, mitigate and repair the damage, and guidance on measures to prevent reoccurrence;
- Obtain professional legal, public relations and IT forensic advice, including assistance in managing the incident, co-ordinating response activities, making representation to regulatory bodies and coordination with law enforcement;
- Crisis communications and public relations costs to manage a reputational crisis, including spokesperson training and social media monitoring;
- Communications to notify affected parties; and
- Remediation services such as credit and identity theft monitoring to protect affected parties from suffering further damages.

**Think Expert. Think iTOO**

**iTOO Special Risks** (Pty) Ltd (Reg No: 2016/281463/07) is an authorised Financial Services Provider (FSP No. 47230).
Underwritten by The Hollard Insurance Company Limited (Reg. No. 1952/003004/06), a Licensed Non-Life Insurer and an authorised Financial Services Provider.

# 1st party cover

| | |
|---|---|
| **Loss of business income** | • Loss of business income and ongoing operational costs following a network breach.<br>• Loss of business income caused by an unintentional system failure that results in a material disruption to the insured's operations.<br>• Loss of business income after systems are deliberately taken offline to contain or manage a cyber incident or comply with Regulator instructions. |
| **Cyber extortion** | Costs to investigate and mitigate a cyber extortion threat including ransom payments and the costs to procure cryptocurrency. |
| **Data restoration** | Costs to restore, replace or recover data that is lost, stolen or corrupt following a cyber incident. |
| **Initial response phase** | A deductible waiver for expenses of specialists to contain and manage an incident, for a pre-determined time without a deductible being applicable. |
| **Theft of funds** | The unrecoverable loss of:<br>• money belonging to the insured, their subsidiaries or senior officers<br>• money the insured is legally responsible for<br>• goods provided by the insured (on a cost price basis)<br>as a direct result of a network breach by a third party or money transferred after receiving a fraudulent payment instruction and following the proper verification process. |
| **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. |
| **Payment card industry** | Cover for fines, penalties, chargebacks and assessments imposed under merchant agreements due to a card data breach. |
| **Outsourced service provider** | Cover for exposure to outsourced IT service providers including:<br>• Initial response phase expenses.<br>• Crisis management and notification expenses.<br>• Data recovery.<br>• Loss of business income.<br>• Disruption and mitigation – costs to change to an alternate outsourced service provider if required. |
| **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. |
| **Post incident betterment** | Cover for costs to improve security posture following an approved claim. |
| **Regulatory fines** | Fines imposed by a government regulatory body due to an information privacy breach. |

# 3rd party cover

| | |
|---|---|
| **Privacy breach 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** | Defence and settlement of liability claims resulting from online content including social media posts or website material, such as defamation, copyright infringement, or privacy violations. |
| **Contingent bodily injury** | Defence and settlement of mental anguish claims caused by a cyber incident. |

**Think Expert. Think iTOO**

**iTOO Special Risks** (Pty) Ltd (Reg No: 2016/281463/07) is an authorised Financial Services Provider (FSP No. 47230).
Underwritten by The Hollard Insurance Company Limited (Reg. No. 1952/003004/06), a Licensed Non-Life Insurer and an authorised Financial Services Provider.