LIABILITY

Non-tangible risks and exposure claims are on the rise. Being the solution providers we are, Howdie offers a comprehensive liability programme that can act as a stand-alone or be combined with our commercial and business offerings.

Changing legislation, multiple lines of exposure from third parties, employees and new cyber disruptor risks have created the need for a 'complete' package. Howdie's liability cover is just that – the complete package – that carry the necessary extensions to safeguard your business today and in the future.

Howdie

COMMERCIAL

CYBER

From the Internet and email to social media and mobility, in our professional and personal lives we are connected and generating data on a daily basis. But while technological and data-processing advances bring opportunities for dynamic growth, efficiency and increased client engagement, and can function as a core business differentiator, our adoption of digital technology has left us more vulnerable than ever to cyber and data risks.

Typical cyber risks include:

- Costs incurred to respond to a data breach
- System unavailability and downtime
- Reputational damage
- Loss of revenue, data and/or competitive advantage
- Loss of investor and/or client confidence
- Litigation arising from compromised systems or data
- Industry and regulatory fines and penalties

Core exposures

- Data/Privacy Breach
- Network Security Breach

WHAT IS COVERED?

First party expenses

- 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.
- Regulatory fines to the extent insurable by law, fines imposed by a government regulatory body due to an information privacy breach.
- Physical damage costs to replace or repair direct physical damage of property due to a system security incident.

LIABILITY

Howdie

COMMERCIAL

Non-tangible risks and exposure claims are on the rise. Being the solution providers we are, Howdie offers a comprehensive liability programme that can act as a stand-alone or be combined with our commercial and business offerings.

Changing legislation, multiple lines of exposure from third parties, employees and new cyber disruptor risks have created the need for a 'complete' package. Howdie's liability cover is just that – the complete package – that carry the necessary extensions to safeguard your business today and in the future.

CYBER

Incident Mitigation:

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

- 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 reoccurrence
- for professional (legal, public relations and IT forensics) advice, including assistance in managing the incident, coordinating response activities, and making representation to regulatory bodies
- 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 credit and identity theft monitoring to protect affected parties from suffering further damages.

Third Party Expenses:

- 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 causing harm to third-party systems and data.
- Media liability defence and settlement of liability claims resulting from disseminated content (including social media content) including unintentional defamation or copyright infringement.

Common causes of incidents include

- Unauthorised access
- Accidents and negligence
- Rogue employees
- Third party access

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 or payment on a fraudulent invoice. Cryptocurrency losses are excluded.

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