Cyber Insurance Policy

February 24, 2021

News: A committee set up by the Insurance Regulatory and Development Authority of India (IRDAI) has recommended the introduction of a cyber insurance policy.

Background

- In October 2020, the IRDAI had set up a committee for cyber liability insurance under P Umesh.
- Amid the Covid-19 pandemic, there has been rising incidences of cyberattacks and a growing number of high-profile data violations.

Data highlighted

- According to the committee report, the number of internet users in India is currently estimated at 700 million.
- India was ranked as the second-largest online market worldwide in 2019, coming second only to China.

The number of internet users is estimated to increase in both urban as well as rural regions. This number is increasing rapidly so also is the number of users of online banking.

Features of an Individual cyber insurance policy

- Theft of Funds, Identity Theft Cover, Social Media cover, Cyber Stalking, Malware Cover, Phishing cover, Data Breach and Privacy Breach Cover, etc

What is cyber insurance?

- A cyber insurance policy, also referred to as cyber risk insurance or cyber liability insurance coverage (CLIC), is designed to help an organization mitigate risk exposure by offsetting costs involved with recovery

after a cyber-related security breach or similar event.

- Although there is no standard for underwriting these policies, the following are common reimbursable expenses:
    - **Investigation:** A forensics investigation is necessary to determine what occurred, how to repair damage and how to prevent the same type of breach from occurring in the future.
    - **Business losses:** A cyber insurance policy may include similar items that are covered by an errors & omissions policy (errors due to negligence and other reasons), as well as monetary losses experienced by network downtime, business interruption, data loss recovery and costs involved in managing a crisis, which may involve repairing reputation damage.
    - **Privacy and notification:** This includes required data breach notifications to customers and other affected parties, which are mandated by law in many jurisdictions, and credit monitoring for customers whose information was or may have been breached.

Lawsuits and extortion: This includes legal expenses associated with the release of confidential information and intellectual property, legal settlements and regulatory fines. This may also include the costs of cyber extortion, such as from ransomware.