Cyber Insurance Policy

Why in News

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

- Cyber insurance policy is a risk transfer mechanism for cyber risk.
  Cyber risk is commonly defined as exposure to harm or loss resulting from breaches of or attacks on information systems.
- This policy will protect the policyholders from **cybercrimes**.

Key Points

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

- **Recommendations:** Cyber insurance policies currently available address requirements of individuals reasonably well. However, there are some areas in the product features and processes which need improvement.
    - **FIR on higher claims:**
        Insurers should not insist on police FIR (First Information Report) for claims upto Rs. 5,000.
            FIR is a critical requirement to assess claims.
    - **Clarity:**
        Clarity in exclusion language relating to compliance with reasonable practices and precautions and need for coverage for bricking costs.
            Bricking refers to a loss of use or functionality of hardware as a result of a cyber event.
    - **On Standardisation of Cyber Insurance Policy:**
        Cyber risks are dynamic and evolving. Standardisation is a good idea but may not be able to address all the emerging risks and is likely to limit innovation.

Cyber Security

- **About**
    - In computers and computer networks, an attack is any attempt to expose, alter, disable, destroy, steal or gain unauthorized access to or make unauthorized use of an asset.
    - A cyberattack is any type of offensive maneuver that targets computer information systems, infrastructures, computer networks, or personal computer devices.
- **Need:**
    According to **Nasscom's Data Security Council of India (DSCI) report 2019,** India witnessed the **second-highest** number of cyber attacks in the world between 2016 and 2018.

- **Ways of Cyberattack:**
  - **Phishing or Spoofing attacks:**

    Spoofing is an identity theft where a person is trying to use the identity of a legitimate user. Phishing is where a person steals the sensitive information of users like bank account details.
  - **Malware or Spyware:**

    Spyware is classified as a type of malware (malicious software) designed to gain access to or damage one's computer, often without one's knowledge. Spyware gathers one's personal information and relays it to advertisers, data firms, or external users.
  - **SIM Swap:**

    Original SIM gets cloned and becomes invalid, and the duplicate SIM can be misused to access the user's online bank account to transfer funds.
  - **Credential Stuffing (compromising devices and stealing data):**

    Credential stuffing is a type of cyberattack where stolen account credentials typically consisting of lists of usernames and/or email addresses and the corresponding passwords are used to gain unauthorized access to user accounts through large-scale automated login requests directed against a web application.
  - **Man-in-the-middle attacks** during online payments or transactions, etc.

- **Government Initiatives to tackle cyber attacks:**
  - **Cyber Surakshit Bharat Initiative:**
    It was launched in 2018 with an aim to spread awareness about cybercrime and building capacity for safety measures for Chief Information Security Officers (CISOs) and frontline IT staff across all government departments.
  - **National Cybersecurity Coordination Centre (NCCC):**
    Its mandate is to scan internet traffic and communication metadata (which are little snippets of information hidden inside each communication) coming into the country to detect real-time cyber threats.
  - **Cyber Swachhta Kendra:**
    In 2017, this platform was introduced for internet users to clean their computers and devices by wiping out viruses and malware.
  - **Information Security Education and Awareness Project (ISEA):**
    A project to raise awareness and to provide research, education and training in the field of Information Security.
  - **National Computer Emergency Response Team** (CERT-In) functions as the nodal agency for coordination of all cyber security efforts, emergency responses, and crisis management.
  - Protection and resilience of critical information infrastructure with the **National Critical Information Infrastructure Protection Centre** (NCIIPC) operating as the nodal agency.
    NCIIPC was created under the Information Technology Act, 2000 to secure India's critical information infrastructure.
  - **Information Technology Act, 2000:**
    The Act regulates use of computers, computer systems, computer networks and also data and information in electronic format.
- **International Mechanisms:**
  - **The International Telecommunication Union** (ITU) : It is a **specialized agency within the United Nations** which plays a leading role in the standardization and development of telecommunications and cyber security issues.
  - **Budapest Convention on Cybercrime:** It is an **international treaty** that seeks to address Internet and computer crime by harmonizing national laws, improving investigative techniques, and increasing cooperation among nations. It came into force on 1st July 2004. **India is not a signatory** to this convention.
  - **Internet Governance Forum** (IGF): It brings together all stakeholders i.e. government, private sector and civil society on the Internet governance debate.

Source:IE