PwC's 2023 Global Risk Survey

For Prelims: Cyber risks, Cybersecurity, Generative Artificial Intelligence, Ransomware Attacks.

For Mains: Challenges Related to Cyber Risk in India, Provisions for Cyber-Security in India.

Source: HT

Why in News?

According to the **Global Risk Survey 2023** by PwC, a global consultancy firm, **Cyber risks** are the biggest threat faced by Indian organizations.

What are the Key Highlights of the Global Risk Survey 2023?

- **Cyber Risks:**
    - Cyber risks are cited as the **biggest threat** faced by Indian organizations, with **38% of respondents feeling highly or extremely exposed to it.**
        - **Climate change** (37%) and **inflation** (36%) rank second and third among the top threats to Indian organizations.
        - **Digital and technology risks** rank fourth, with 35% of Indian business leaders concerned about these risks.
- **Risk Management:**
    - Indian organizations are proactively **investing in** cybersecurity, with over half planning investments in cybersecurity tools (55%) and AI-related technologies (55%) in the next 1–3 years, aligning with global trends (51% and 49%, respectively).
    - To reinforce these investments, **71% of Indian organizations are actively leveraging cybersecurity and IT data for risk management** and opportunity identification, surpassing the global average of 61%.
    - The survey also revealed how organizations are using emerging technologies such as **Generative Artificial Intelligence** for risk management, with **48% of Indian enterprises** having deployed AI and machine learning for automated risk assessment and response to a large extent. This is slightly lower than the global response of 50%.
        - This strategic approach signifies a commitment to fortify cybersecurity defences and embrace evolving technologies for resilience.
- **Legacy Technologies:**
    - 42% of Indian organizations grapple with heightened **security vulnerabilities attributed to legacy technologies** (Outdated technology systems and infrastructure), surpassing the global average of 36%.
    - Moreover, 46% of Indian companies face increased maintenance costs due to legacy tech, limiting budgets for innovative risk solutions, exceeding the global figure of 39%.
- **Resilience Investments:**
    - **88% of Indian organizations have actively invested** in resilience building over the past year, surpassing the global average of 77%.
        - Resilience Investments include a resilience team, comprising members from

functions such as business continuity, cyber, crisis management and risk management to swiftly respond to risk events as they occur.

Why are Cyber Risks a Primary Threat to Indian Organizations?

- Cyber risks, encompassing malware**,** trojans, and **spyware**, have prominently emerged as the foremost threat for Indian organizations, notably highlighted by a substantial increase in **ransomware attacks.**
  - Despite containment, such risks significantly **impact market perception**, influencing **stock prices and eroding trust.**
- Companies paying the ransom witnessed a **doubling of the cost of data recovery** compared to those relying on backups, emphasizing the financial toll of succumbing to ransomware demands.
- IT organizations store a **diverse range of critical data, encompassing personally identifiable information, intellectual property, access credentials, and financial data.**
  - This multi-dimensional data provides threat actors with leverage to execute and perpetuate a range of **malicious activities.**
  - Leaked data, especially intellectual property, can lead to **devaluation and replication of software,** posing a severe threat to revenue streams.
- The data's intrinsic value and potential impact on the organization's stakeholders increase the likelihood of successful ransom collection.

Laws Addressing Cyber Risks for Indian Organizations:

- **The Information Technology (IT) Act, of 2000:**
  - It is the primary legislation dealing with cybersecurity, data protection and cybercrime. Identifying activities such as hacking, denial-of-service attacks, phishing, malware attacks, identity fraud and electronic theft as punishable offences.
- **Digital Personal Data Protection (DPDP) Act, 2023:**
  - The **DPDP Act, 2023** is legislation acknowledging **individuals' right to protect their digital personal data** while emphasizing the lawful processing of such data for legitimate purposes
    - It imposes accountability and responsibilities on data processors. The DPDP Act, 2023 addresses concerns about the use of personal data by employees and customers, fostering a higher standard of data privacy.
- **National Cyber Security Policy 2013**:
  - It is designed to safeguard information and infrastructure in cyberspace by building capabilities for threat prevention and response, reducing vulnerabilities, and strengthening national security digitally.
  - It focuses on ensuring a secure **computing environment, fostering trust in electronic transactions**, and guiding stakeholders' actions for **cyberspace protection.**
- **National Cyber Security Strategy 2020:**
  - Aims to improve cyber awareness and cybersecurity through more stringent audits. Empanelled cyber auditors will look more carefully at the security features of organizations than are legally necessary now.

UPSC Civil Services Examination, Previous Year Question (PYQ)

Prelims

Q.1 In India, it is legally mandatory for which of the following to report on cyber security incidents? (2017)

1. Service providers
2. Data centres
3. Body corporate

Select the correct answer using the code given below:

(a) 1 only
(b) 1 and 2 only
(c) 3 only
(d) 1, 2 and 3

Ans: (d)

Mains

Q. What are the different elements of cyber security? Keeping in view the challenges in cyber security, examine the extent to which India has successfully developed a comprehensive National Cyber Security Strategy. **(2022)**

PDF Refernece URL: https://www.drishtiias.com/printpdf/pwc-s-2023-global-risk-survey