Science & Technology · GS - III

Third-party service providers have emerged as critical vulnerabilities in the cybersecurity architecture of financial institutions. Examine the implications of supply-chain cyberattacks for India's digital financial ecosystem and suggest measures to strengthen resilience.

EXAM YEAR	PAPER	SUBJECT
DAILY PRACTICE 20/11/2026	GS - III	Science & Technology

MARKS	WORD LIMIT
15	~250 words

Answer Hint

Third-party risk, supply-chain attacks, financial cybersecurity, RBI regulations, data protection, CERT-In, digital payments, vendor audits, incident reporting, cyber resilience.

Model Answer

Introduction

The reported data leak involving JPMorgan Chase, Visa and Mastercard through third-party service providers highlights the growing risks of supply-chain cyberattacks. Financial institutions must therefore secure not only their internal systems but also their external technology partners.

Implications for India's Digital Financial Ecosystem

1. Customer Data Exposure

- Leakage of email addresses and phone numbers can facilitate phishing, identity fraud and social engineering.
- Misuse of personal information can undermine consumer trust in digital banking and payments.

2. Supply-Chain Vulnerabilities

- Weak cybersecurity among vendors can expose otherwise secure financial institutions.
- Dependence on cloud platforms, marketing agencies and technology providers expands the attack surface.

3. Financial and Systemic Risks

- Cyber incidents can disrupt financial services and damage institutional credibility.
- Coordinated attacks on critical financial infrastructure may affect public confidence in digital transactions.

Measures to Strengthen Cyber Resilience

- **Regulatory oversight:** Strengthen RBI's cybersecurity and third-party risk management requirements.
- **Vendor accountability:** Conduct regular security audits, vulnerability assessments and contractual compliance checks.
- **Data protection:** Implement encryption, access controls and data-minimisation practices.
- **Incident response:** Strengthen CERT-In coordination, timely reporting and threat intelligence sharing.
- **Consumer awareness:** Promote phishing awareness and secure authentication practices.

Conclusion

Cybersecurity in finance must adopt an ecosystem-wide approach rather than focusing exclusively on internal infrastructure. Strong vendor accountability, regulatory supervision and rapid incident response are essential for maintaining trust in India's digital financial system.

BECOME IAS
AI-POWERED UPSC PREP