Defence & Security · GS - III

Examine the vulnerabilities of digital information infrastructure to cyberattacks and suggest measures to strengthen its resilience.

EXAM YEAR	PAPER	SUBJECT
DAILY PRACTICE 27/11/2026	GS - III	Defence & Security

MARKS	WORD LIMIT
15	~250 words

Answer Hint

Critical information infrastructure, ransomware, data integrity, business continuity, incident response, cyber hygiene, public-private coordination, CERT-In

Model Answer

Digital information infrastructure supports communication, financial transactions, public administration and the functioning of modern media. The cyberattack on Agence France-Presse (AFP), which led to the temporary shutdown of its AFP Forum platform, illustrates how disruption of a digital service can affect an organisation's wider network of users.

Nature of vulnerabilities

1. **System intrusion:** Weak authentication, unpatched software and compromised credentials can provide attackers access to digital platforms.
2. **Service disruption:** Distributed denial-of-service attacks, ransomware and other malicious activities can interrupt essential services.
3. **Data compromise:** Cyber intrusions may threaten confidentiality, integrity and availability of information.
4. **Supply-chain exposure:** Third-party vendors and interconnected platforms can become entry points for attacks, extending their impact beyond the initial victim.

Resilience requirements

1. **Technical safeguards:** Multi-factor authentication, encryption, regular security audits and timely software updates should be institutionalised.
2. **Operational preparedness:** Organisations need tested backup systems, disaster-recovery arrangements and alternative delivery channels.
3. **Institutional coordination:** CERT-In, sectoral regulators and private cybersecurity experts should facilitate timely incident reporting and threat intelligence sharing.
4. **Skilled workforce:** Regular cyber drills and employee awareness programmes can reduce human-related vulnerabilities.
5. **Accountability:** Forensic investigation and evidence preservation are essential for identifying attack methods and supporting lawful action.

Indian context: The Information Technology Act, 2000, and the National Critical Information Infrastructure Protection Centre provide important elements of India's cybersecurity framework.

Digital resilience requires more than preventing intrusions; it demands the capacity to detect, contain and recover from attacks while maintaining essential services.

BECOME IAS
AI POWERED UPSC PREP