Defence & Security · GS - III

Discuss the potential threats of Cyber attack and the security framework to prevent it.

EXAM YEAR	PAPER	SUBJECT
2017	GS - III	Defence & Security

MARKS	WORD LIMIT
10	~150 words

Answer Hint

Critical information infrastructure; ransomware; data breaches; cyber espionage; CERT-In; NCIIPC; cyber resilience

Model Answer

Introduction

Cyberattacks exploit digital vulnerabilities to disrupt services, steal information or compromise national security. India's growing dependence on digital systems makes cybersecurity a critical governance and security priority.

Potential Threats

- **Critical infrastructure attacks:** Power grids, banking, telecommunications and transport systems may face disruption.
- **Data theft:** Personal, financial and government information can be stolen or misused.
- **Ransomware:** Malicious software can lock systems and demand payment.
- **Cyber espionage:** Attackers may access sensitive government, defence or commercial information.
- **Disinformation:** Coordinated digital campaigns can undermine public trust and social stability.
- **Supply-chain attacks:** Compromised software or service providers can expose multiple organisations.

Security Framework in India

- **CERT-In:** The Indian Computer Emergency Response Team issues advisories, coordinates incident response and supports cybersecurity preparedness.
- **NCIIPC:** The National Critical Information Infrastructure Protection Centre focuses on protecting designated critical information infrastructure.
- **Information Technology Act, 2000:** Provides a legal framework addressing cyber offences and electronic systems.
- **National Cyber Coordination Centre:** Supports situational awareness and coordination concerning cyber threats.
- **Sectoral safeguards:** Regulators and organisations establish security controls, incident reporting and resilience measures.

Measures for Strengthening Security

Adopt regular security audits, multi-factor authentication, encryption, employee training, incident-response exercises and reliable backup systems. Improve international cooperation and develop specialised cyber skills.

Conclusion

Cybersecurity requires coordinated action by government, industry and citizens. Prevention, rapid incident response and resilient digital infrastructure are essential to protect national security and public trust.

BECOME IAS
AI POWERED UPSC PREP