Science & Technology · GS - III

Examine the vulnerabilities of government databases and digital law-enforcement systems to cyberattacks. Suggest measures to strengthen India's cybersecurity architecture and protect sensitive public data.

EXAM YEAR	PAPER	SUBJECT
DAILY PRACTICE 21/11/2026	GS - III	Science & Technology

MARKS	WORD LIMIT
15	~250 words

Answer Hint

Critical information infrastructure, confidentiality-integrity-availability, ransomware, insider threats, zero-trust architecture, CERT-In, NCIIPC, data protection, cyber forensics, inter-agency coordination, capacity building.

Model Answer

Introduction

The increasing digitisation of governance and policing has made government databases essential to public administration and national security. Cyberattacks targeting such systems can compromise sensitive information and disrupt critical law-enforcement functions.

Major Vulnerabilities

1. **Centralised databases:** Large repositories of criminal records and identity information become attractive targets for cybercriminals.

2. **Legacy infrastructure:** Outdated software, inadequate encryption and unpatched systems create exploitable security gaps.

3. **Insider threats:** Misuse of privileged access by employees or contractors can compromise confidential information.

4. **Supply-chain risks:** Third-party vendors and interconnected digital platforms may provide entry points for attackers.

5. **Operational disruption:** Manipulation or unavailability of criminal records can affect investigations, verification, warrants and public safety.

Measures to Strengthen Cybersecurity

- **Institutional coordination:** Strengthen the roles of CERT-In and NCIIPC in incident response and critical infrastructure protection.
- **Zero-trust security:** Adopt continuous authentication, least-privilege access and multi-factor authentication.
- **Data protection:** Apply encryption, secure backups, access logs and regular security audits.
- **Capacity building:** Develop cyber-forensic capabilities and train law-enforcement personnel.
- **Incident preparedness:** Conduct vulnerability assessments, penetration testing and periodic cyberattack simulations.
- **Legal accountability:** Ensure compliance with applicable cybersecurity and data-protection frameworks.

Conclusion

Cybersecurity is an essential component of national security and effective digital governance. A resilient architecture combining technological safeguards, skilled personnel, institutional coordination and accountability is necessary to protect sensitive government databases and maintain public trust.

BECOME IAS
AI POWERED UPSC PREP