# Digital Threat Report 2024

**For Prelims**: **Digital threats**, **Artificial Intelligence, Deep fakes**, **WannaCry ransomware attack**, **Phishing, Internet of Things**, **National Cyber Security Policy**, **Indian Cyber Crime Coordination Centre**, **Computer Emergency Response Team - India** , **Cyber Swachhta Kendra** , **Digital Personal Data Protection Act 2023.**

**For Mains:** Key Highlights of Digital Threat Report 2024, Key Recommendations for Cyber Security in BFSI sector, Current Major Cyber Threats that India is Facing, Key Government Initiatives Related to Cybersecurity in India.

**Source: PIB**

## Why in News?

India has released its first-ever **Digital Threat Report 2024,** aimed at **strengthening cybersecurity** in the **Banking, Financial Services, and Insurance (BFSI) sector.** The report highlights **evolving cyber risks and outlines strategic measures** to protect the nation's financial infrastructure, crucial for its digital economy.

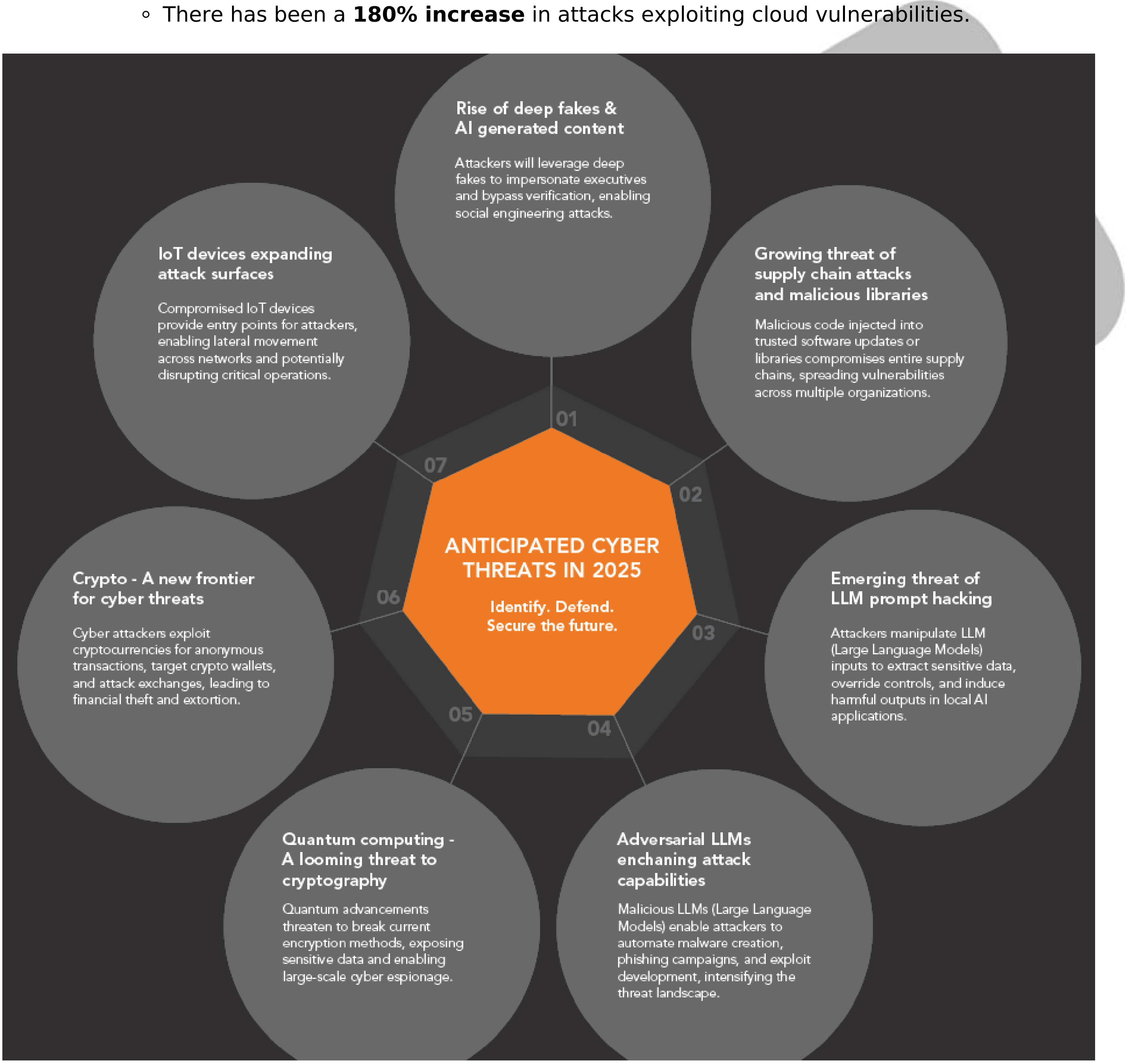
### What is the Digital Threat Report 2024?

- The **Digital Threat Report 2024** is a collaborative initiative by **SISA (Strategic Information Services Agreement),** a global cybersecurity firm, along with the **Computer Emergency Response Team (CERT-In),** and **CSIRT-Fin**.
- It provides a **comprehensive analysis of the escalating cybersecurity risks** within **India's BFSI** sector and guides organizations to adopt **stronger security measures, improve compliance protocols, and enhance threat detection capabilities.**

## What are the Key Highlights of the Cyber Threat Report 2024?

- **Surge in Cyberattacks and Data Breach Costs**: In 2024, the **BFSI** sector witnessed a surge in **cyberattacks,** with global data breach costs rising to **USD 4.88 million** (a **10% increase** from 2023) and **USD 2.18 million** in India.
  - **BFSI's digital growth**, projected to reach **USD 3.1 trillion in payments by 2028**, is widening its cyber threat exposure.
  - **Phishing attacks** in India surged by **175%** in June 2024 compared to 2023.
- **Crypto Attacks: Crypto exchanges** have been targeted by cybercriminals and new **malware variants** also threaten crypto wallets by **extracting private keys for unauthorized access.**
- **Social Engineering Attacks**: **Business Email Compromise (BEC)** and **phishing** are rising cyber threats, with **54% of BEC cases involving pretexting**.

    - **AI** and **deepfake technologies** are making these attacks more convincing by impersonating executives to manipulate financial transactions or steal sensitive data.
- **Impact of AI on Phishing**: AI is making phishing attacks more convincing by generating emails that mimic trusted entity's tone, style, and branding.
    - AI-driven **chatbot phishing scams** engage victims interactively to extract personal data.
    - Large language models (LLMs) like **WormGPT** and **FraudGPT bots** are lowering the barrier for cybercriminals, enabling the **creation of more convincing phishing emails and malware.**
- **Stolen Credentials and Malware**: **Hackers** are using **stolen login details and malware** using techniques like **session hijacking**, brute-force attacks, **deepfake technology**, and **BOLA** vulnerabilities to **bypass** Multi-Factor Authentication (MFA), mainly targeting **SaaS platforms** like email and VPN services.
    - **SaaS platforms** are a type of digital platform that facilitates the **selling, distribution, and management of cloud-based software and services.**
- **Cloud Security Weaknesses**: Misconfigured cloud services, such as publicly accessible storage and weak access controls, are major targets.
    - There has been a **180% increase** in attacks exploiting cloud vulnerabilities.



ANTICIPATED CYBER THREATS IN 2025

Identify. Defend. Secure the future.

01 Rise of deep fakes & AI generated content

Attackers will leverage deep fakes to impersonate executives and bypass verification, enabling social engineering attacks.

02 Growing threat of supply chain attacks and malicious libraries

Malicious code injected into trusted software updates or libraries compromises entire supply chains, spreading vulnerabilities across multiple organizations.

03 Emerging threat of LLM prompt hacking

Attackers manipulate LLM (Large Language Models) inputs to extract sensitive data, override controls, and induce harmful outputs in local AI applications.

04 Adversarial LLMs enchaning attack capabilities

Malicious LLMs (Large Language Models) enable attackers to automate malware creation, phishing campaigns, and exploit development, intensifying the threat landscape.

05 Quantum computing - A looming threat to cryptography

Quantum advancements threaten to break current encryption methods, exposing sensitive data and enabling large-scale cyber espionage.

06 Crypto - A new frontier for cyber threats

Cyber attackers exploit cryptocurrencies for anonymous transactions, target crypto wallets, and attack exchanges, leading to financial theft and extortion.

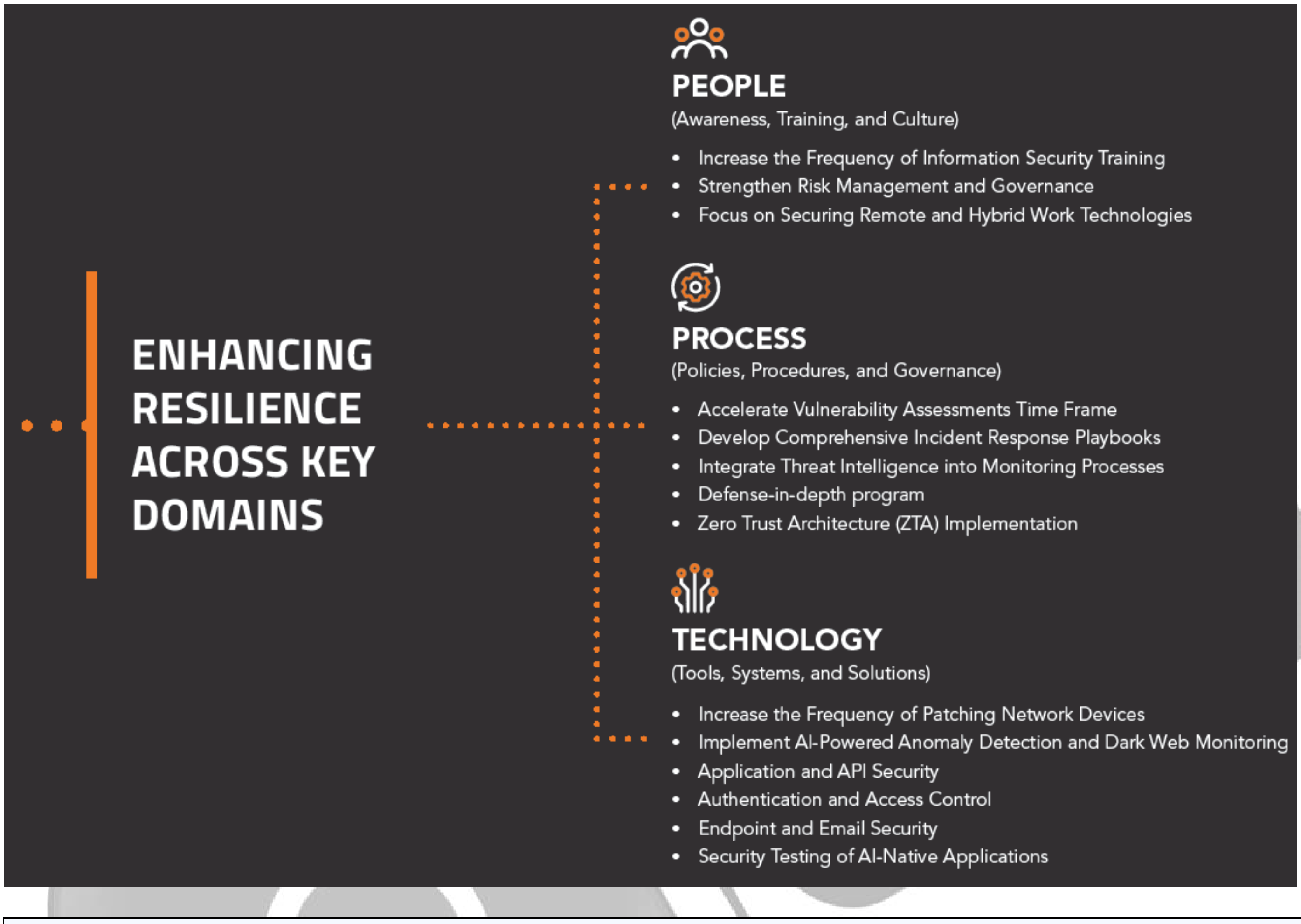
07 IoT devices expanding attack surfaces

Compromised IoT devices provide entry points for attackers, enabling lateral movement across networks and potentially disrupting critical operations.

- **Key Recommendations:**
    - It includes adopting a **human-centric, leadership-driven approach** to cybersecurity,

backed by continuous employee training and cyber-awareness to counter emerging threats like **AI phishing and deepfakes.**

- Implement **regular Automated Vulnerability Scans**, **real-time threat intelligence sharing**, and a **multi-layered "defense-in-depth" strategy** with f**irewalls, endpoint protection** and **Zero Trust architecture.**
- Leveraging Technology to ensure **timely patching (updates), AI-based threat detection** and use of **MFA for access control**.



ENHANCING RESILIENCE ACROSS KEY DOMAINS

**PEOPLE**

(Awareness, Training, and Culture)

- Increase the Frequency of Information Security Training
- Strengthen Risk Management and Governance
- Focus on Securing Remote and Hybrid Work Technologies

**PROCESS**

(Policies, Procedures, and Governance)

- Accelerate Vulnerability Assessments Time Frame
- Develop Comprehensive Incident Response Playbooks
- Integrate Threat Intelligence into Monitoring Processes
- Defense-in-depth program
- Zero Trust Architecture (ZTA) Implementation

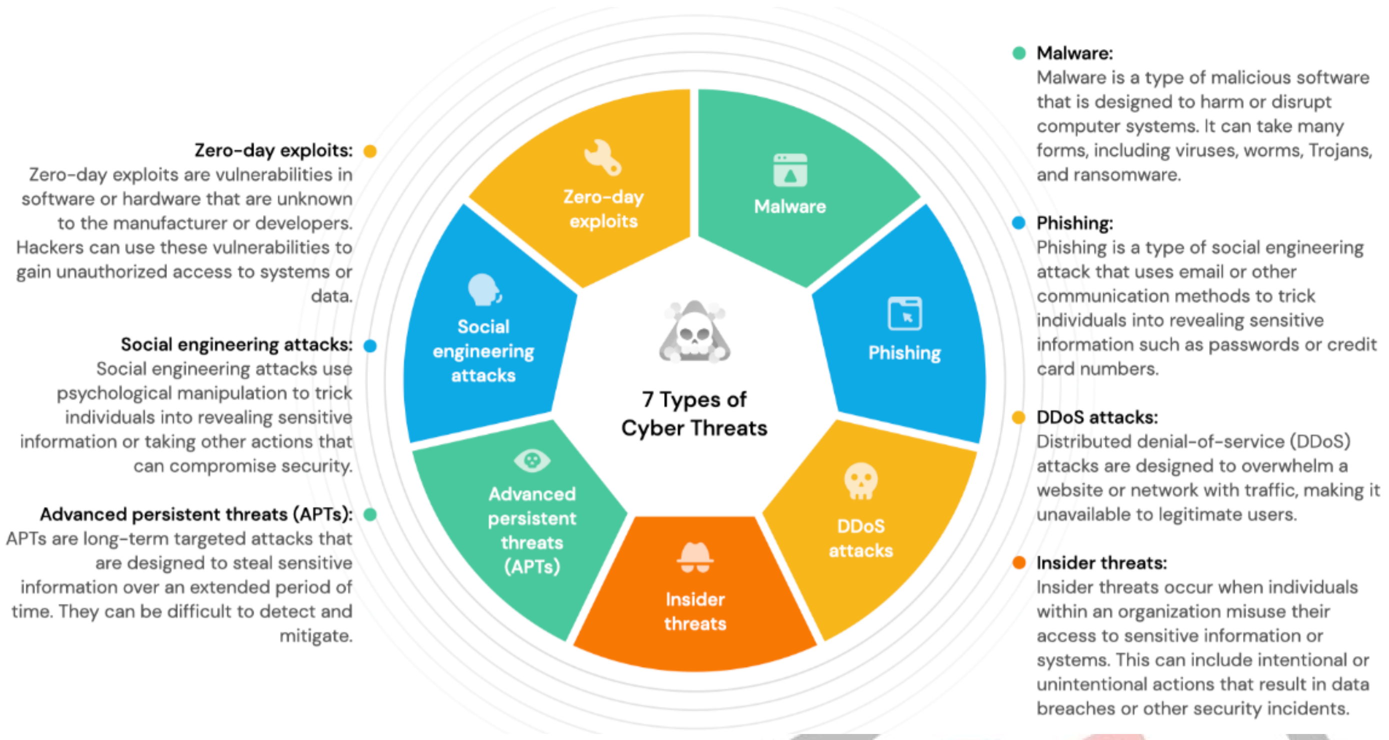
**TECHNOLOGY**

(Tools, Systems, and Solutions)

- Increase the Frequency of Patching Network Devices
- Implement AI-Powered Anomaly Detection and Dark Web Monitoring
- Application and API Security
- Authentication and Access Control
- Endpoint and Email Security
- Security Testing of AI-Native Applications

### What are the Key Emerging Cyber Threats in India?

**Click Here to Read: Key Cyber Threats in India**



**Zero-day exploits:** Zero-day exploits are vulnerabilities in software or hardware that are unknown to the manufacturer or developers. Hackers can use these vulnerabilities to gain unauthorized access to systems or data.

**Social engineering attacks:** Social engineering attacks use psychological manipulation to trick individuals into revealing sensitive information or taking other actions that can compromise security.

**Advanced persistent threats (APTs):** APTs are long-term targeted attacks that are designed to steal sensitive information over an extended period of time. They can be difficult to detect and mitigate.

**Malware:** Malware is a type of malicious software that is designed to harm or disrupt computer systems. It can take many forms, including viruses, worms, Trojans, and ransomware.

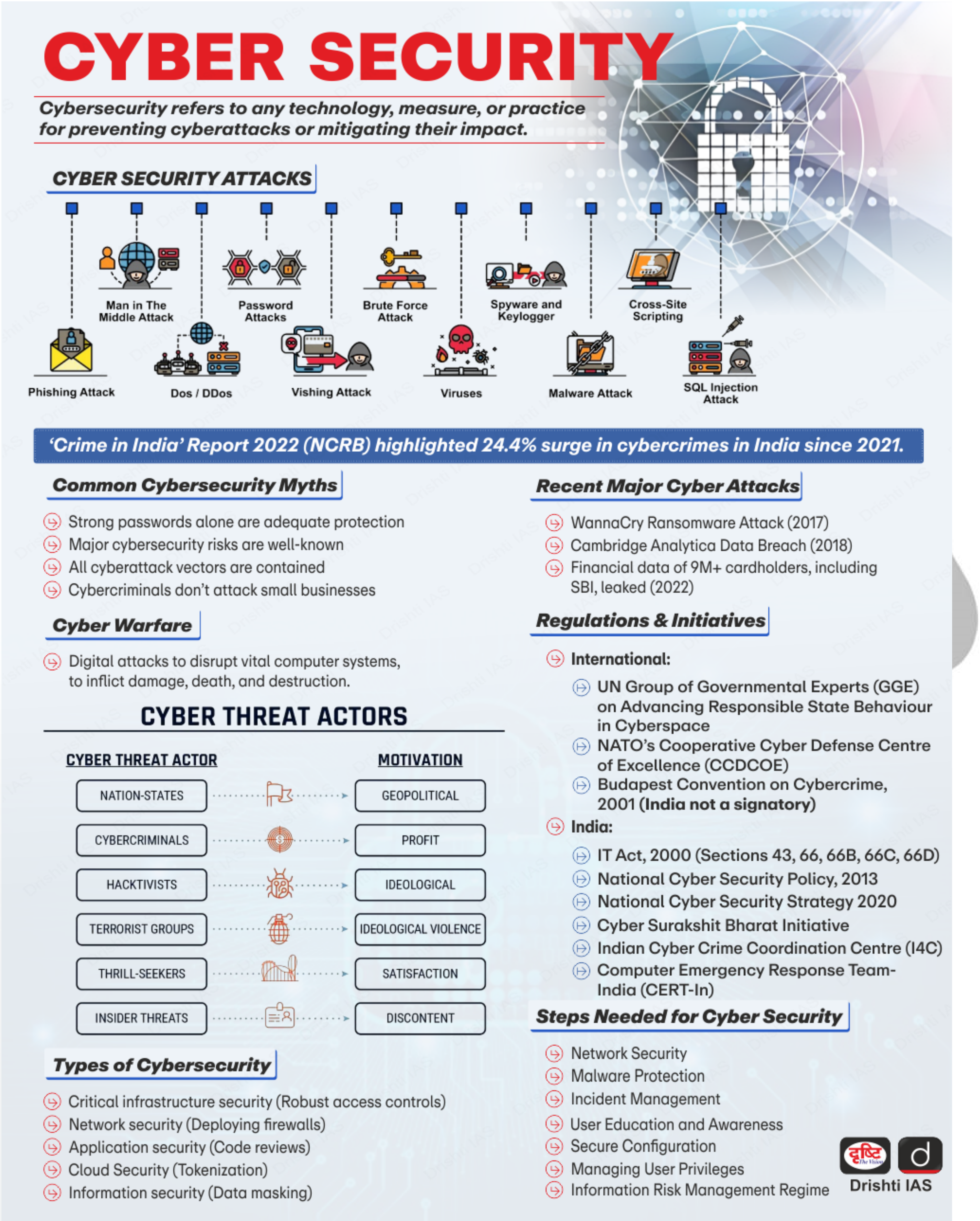
**Phishing:** Phishing is a type of social engineering attack that uses email or other communication methods to trick individuals into revealing sensitive information such as passwords or credit card numbers.

**DDoS attacks:** Distributed denial-of-service (DDoS) attacks are designed to overwhelm a website or network with traffic, making it unavailable to legitimate users.

**Insider threats:** Insider threats occur when individuals within an organization misuse their access to sensitive information or systems. This can include intentional or unintentional actions that result in data breaches or other security incidents.

## What is the Current Framework for Cybersecurity in India?

- **Legislative Measures:**
  - [Information Technology Act, 2000 (IT Act)]
  - [Digital Personal Data Protection Act, 2023]
- **Institutional Framework:**
  - Indian Computer Emergency Response Team **(CERT-In)**
  - National Critical Information Infrastructure Protection Centre **(NCIIPC)**
  - Indian Cyber Crime Coordination Centre **(I4C)**
  - Cyber Swachhta Kendra
- **Strategic Initiatives:**
  - Bharat National Cybersecurity Exercise 2024
  - **National Cyber Security Policy, 2013:** Provides vision and strategies for securing cyberspace and protecting critical information infrastructure.



# CYBER SECURITY

*Cybersecurity refers to any technology, measure, or practice for preventing cyberattacks or mitigating their impact.*

## CYBER SECURITY ATTACKS

Phishing Attack
Man in The Middle Attack
Dos / DDos
Password Attacks
Vishing Attack
Brute Force Attack
Viruses
Spyware and Keylogger
Malware Attack
Cross-Site Scripting
SQL Injection Attack

**'Crime in India' Report 2022 (NCRB) highlighted 24.4% surge in cybercrimes in India since 2021.**

### Common Cybersecurity Myths

- Strong passwords alone are adequate protection
- Major cybersecurity risks are well-known
- All cyberattack vectors are contained
- Cybercriminals don't attack small businesses

### Cyber Warfare

- Digital attacks to disrupt vital computer systems, to inflict damage, death, and destruction.

## CYBER THREAT ACTORS

| CYBER THREAT ACTOR | MOTIVATION |
|---|---|
| NATION-STATES | GEOPOLITICAL |
| CYBERCRIMINALS | PROFIT |
| HACKTIVISTS | IDEOLOGICAL |
| TERRORIST GROUPS | IDEOLOGICAL VIOLENCE |
| THRILL-SEEKERS | SATISFACTION |
| INSIDER THREATS | DISCONTENT |

### Types of Cybersecurity

- Critical infrastructure security (Robust access controls)
- Network security (Deploying firewalls)
- Application security (Code reviews)
- Cloud Security (Tokenization)
- Information security (Data masking)

### Recent Major Cyber Attacks

- WannaCry Ransomware Attack (2017)
- Cambridge Analytica Data Breach (2018)
- Financial data of 9M+ cardholders, including SBI, leaked (2022)

### Regulations & Initiatives

- **International:**
  - UN Group of Governmental Experts (GGE) on Advancing Responsible State Behaviour in Cyberspace
  - NATO's Cooperative Cyber Defense Centre of Excellence (CCDCOE)
  - Budapest Convention on Cybercrime, 2001 **(India not a signatory)**
- **India:**
  - IT Act, 2000 (Sections 43, 66, 66B, 66C, 66D)
  - National Cyber Security Policy, 2013
  - National Cyber Security Strategy 2020
  - Cyber Surakshit Bharat Initiative
  - Indian Cyber Crime Coordination Centre (I4C)
  - Computer Emergency Response Team-India (CERT-In)

### Steps Needed for Cyber Security

- Network Security
- Malware Protection
- Incident Management
- User Education and Awareness
- Secure Configuration
- Managing User Privileges
- Information Risk Management Regime

Drishti IAS

## Conclusion

As cyber threats evolve, adopting a **proactive, multi-layered cybersecurity approach** is crucial for safeguarding critical infrastructure. Prioritizing **early vulnerability assessments, AI-driven detection, strong authentication,** and **securing applications enhances resilience.** Embedding cybersecurity into **organizational strategies** will strengthen India's digital ecosystem and ensure long-term security.

***Drishti Mains Question:***

What are the key challenges posed by Cyber Attacks on india. How can the government formulate effective strategies to mitigate the risks posed by cyber attacks?

## UPSC Civil Services Examination, Previous Year Question (PYQ)

### ***Prelims***

**Q.1 In India, under cyber insurance for individuals, which of the following benefits are generally covered, in addition to payment for the loss of funds and other benefits? (2020)**

1. Cost of restoration of the computer system in case of malware disrupting access to one's computer
2. Cost of a new computer if some miscreant wilfully damages it, if proved so
3. Cost of hiring a specialised consultant to minimise the loss in case of cyber extortion
4. Cost of defence in the Court of Law if any third party files a suit

**Select the correct answer using the code given below:**

(a) 1, 2 and 4 only
(b) 1, 3 and 4 only
(c) 2 and 3 only
(d) 1, 2, 3 and 4

**Ans: (b)**

**Q.2 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)