



## Ransomware Attack Disrupts Bank Operations

**For Prelims:** [Ransomware](#), [Regional Rural Banks](#), [National Payments Corporation of India](#), [Unified Payments Interface](#), [Aadhaar-enabled payment systems](#), [Malware](#)

**For Mains:** Impact of Ransomware on the Financial Sector, Cybersecurity Measures, Government Initiatives

**Source:** [IE](#)

### Why in News?

Recently, a [ransomware attack](#) severely disrupted the operations of at least 150-200 [cooperative banks](#) and [Regional Rural Banks \(RRBs\)](#) in India.

- The [National Payments Corporation of India \(NPCI\)](#) has identified the attack, which has primarily affected banks serviced by **C-Edge Technologies Ltd.**, a joint venture between **Tata Consultancy Services Ltd. (TCS)** and [State Bank of India \(SBI\)](#).

### How has the Ransomware Attack Affected the Banks?

- The ransomware attack targeted C-Edge Technologies Ltd., impacting their ability to provide services to cooperative banks and RRBs.
  - Customers of the affected banks were unable to access payment systems, including [Unified Payments Interface \(UPI\)](#) and [Aadhaar-enabled payment systems \(AePS\)](#).
  - Some RRBs, depending on their sponsor banks, continued to function normally as they use different technology service providers.
- **Broader Implications for the Payment Ecosystem:**
  - The attack highlights the **vulnerability of technology service providers** and their critical role in maintaining the payment infrastructure.
  - The incident underscores the **need for robust [cybersecurity measures](#)** to protect against such attacks in the future.
  - Cooperation between NPCI, banks, and technology providers is crucial to swiftly address and mitigate the impacts of such disruptions.

**Note:** AePS is a bank-led model that allows **online interoperable financial transactions** at Point of Sale (PoS) or micro-ATMs through the Business Correspondent of any bank using **Aadhaar authentication**.

- It was taken up by NPCI, a joint initiative of [Reserve Bank of India \(RBI\)](#) and [Indian Banks' Association \(IBA\)](#) to provide easy and secure access to banking services for the poor and marginalised, especially in rural and remote areas.

## What is Ransomware?

- **Definition: Ransomware is a type of [malware](#)** that encrypts a victim's data or locks their device, demanding a ransom for the decryption key or to regain access.
- **Early Attacks:** Initially, ransomware attacks focused on **encrypting data and demanding a ransom for the decryption key.**
- **Modern Tactics:** Recent ransomware attacks have evolved to include double-extortion and triple-extortion tactics:
  - **Double-extortion:** Attackers threaten to leak stolen data online if the ransom is not paid.
  - **Triple-extortion:** Attackers use stolen data to target the victim's customers or business partners.
- **Types of Ransomware:**
  - **Encrypting Ransomware (Crypto Ransomware):** Encrypts the victim's data, demanding a ransom for the decryption key.
  - **Non-encrypting Ransomware (Screen-locking Ransomware):** Locks the victim's entire device, displaying a ransom demand on the screen.
  - **Subcategories of Ransomware Include:**
    - **Leakware or Doxware:** Steals and threatens to publish sensitive data.
    - **Mobile Ransomware:** Affects mobile devices, often using screen-lockers.
    - **Wipers:** Threaten to destroy data, sometimes even if the ransom is paid.
    - **Scareware:** Uses fear tactics to coerce payment, sometimes posing as legitimate alerts.
- **Ransomware as Cyber Threat:**
  - **Financial Impact:** Ransomware attacks can cost organisations millions of dollars.
    - An IBM (International Business Machines Corporation) report showed that the **average cost of a data breach touched an all-time high of Rs 19.5 crore (USD 2.35 million)** in financial year 2024, up by around 7% over 2023, with the local industrial sector being the most impacted.
    - Ransomware victims and negotiators are reluctant to disclose ransom payments.
  - **Speed of Attacks:** Once hackers gain access to a network, they can deploy ransomware in **less than four days**, giving organisations **little time to detect and respond.**
- **Steps for Responding to a Ransomware:**
  - **Isolate the infected device from the network** to contain the infection. Disconnect all suspiciously behaving devices from the network to stop the spread of infection.
  - Identify the **entry point by checking for any alerts** from any active monitoring platform and identify the ransomware by scanning encrypted files and ransom notes.
  - **Prioritize the restoration of systems** by restoring the most critical ones first, followed by eradication of the threat from the network.
    - If backup is available, restore the systems from a backup. **Otherwise, try for decryption options.**

## How does Ransomware Infect Systems?

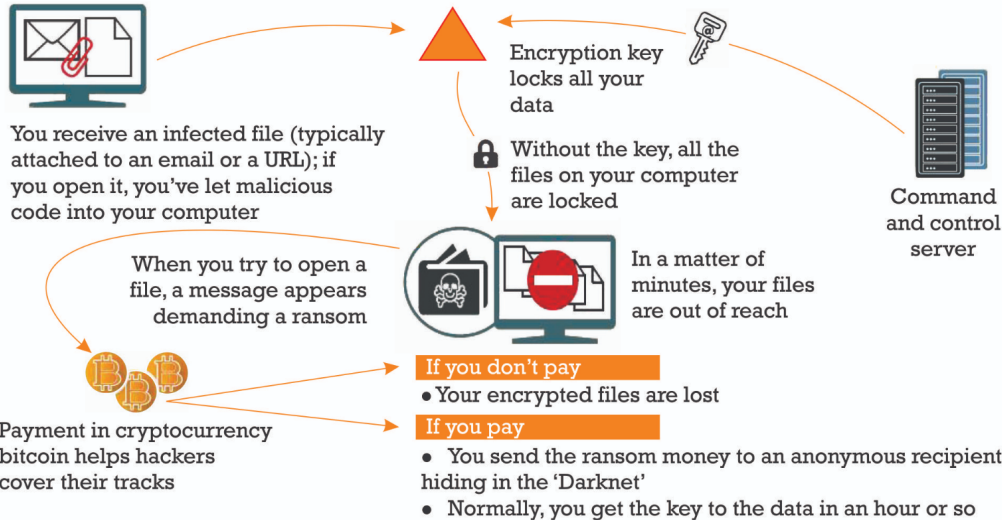
- **Phishing:** It is a type of cyberattack that uses [Social Engineering tricks](#) to deceive victims into downloading ransomware through malicious attachments or links.
  - Social engineering is the use of psychological manipulation to trick users into making security mistakes or revealing sensitive information.
- **Exploiting Vulnerabilities:** Uses existing or [zero-day vulnerabilities](#) to inject ransomware.
- **Credential Theft:** Steals authorised user credentials to deploy ransomware.
- **Other Malware:** Use other malware (e.g., [Trojans](#)) to spread ransomware.
- **Drive-by Downloads:** Infects devices through compromised websites.
- **Ransomware as a Service (RaaS):** Allows cybercriminals to use ransomware developed by others in exchange for a share of the ransom.

### Notable Ransomware Variants

- [Akira Ransomware](#)
- [LockBit Ransomware](#)
- **CryptoLocker:** Credited with kick-starting the modern age of ransomware in 2013.

- **WannaCry:** A cryptoworm that attacked over 200,000 computers in 150 countries in 2017.
- **Petya and NotPetya:** Encrypts the file system table, rendering computers unable to boot.
- **Ryuk:** Popularized big-game ransomware attacks against high-value targets.
- **DarkSide:** Responsible for the Colonial Pipeline attack in 2021.
- **Locky:** Uses macros in email attachments to infect devices.
- **REvil:** Known for big-game hunting and double-extortion attacks.
- **Conti:** Operated a RaaS scheme, using double-extortion tactics.

// **HOW RANSOMWARE WORKS** Malicious code blocks access to the data in your computer



WHAT IS RANSOMWARE	HOW THE HACKERS STRUCK	GOVT AGENCIES/COMPANIES AFFECTED GLOBALLY
<ul style="list-style-type: none"> <li>❖ The malware shutting down computers worldwide is <b>known as WannaCry</b> and variants of that name</li> <li>❖ This type of malware is <b>called ransomware as it first scrambles a victim's files and then demands a payment</b> to unscramble them</li> </ul>	<ul style="list-style-type: none"> <li>❖ The ransomware exploits a weakness in Microsoft Windows systems that was identified by the US National Security Agency and given the name 'EternalBlue'</li> <li>❖ But NSA's code was among a cache stolen by a hackers' group known as The Shadow Brokers, who then attempted to sell it in an online auction</li> </ul>	<ul style="list-style-type: none"> <li>❖ Britain's National Health Service (NHS)</li> <li>❖ Russian interior ministry (about 1,000 computers)</li> <li>❖ Spain's communications giant Telefonica</li> <li>❖ Spain's power firm Iberdrola</li> <li>❖ FedEx in the US</li> <li>❖ Japanese carmaker Nissan's plant in England</li> <li>❖ German rail operator Deutsche Bahn</li> <li>❖ French automaker Renault halted production at several sites in Europe</li> </ul>
<p><b>HOW DOES IT WORK</b></p> <ul style="list-style-type: none"> <li>❖ WannaCry seems to be deployed via a worm — a programme that spread by itself between computers</li> <li>❖ Once malware is inside an organisation, it will find vulnerable machines and infect them too</li> <li>❖ Infections reported in 150 countries, including Russia and China. In UK, hospital systems badly hit</li> </ul>	<p><b>How They FELL FOR IT</b></p> <ul style="list-style-type: none"> <li>❖ Cyber extortionists tricked victims into opening malicious attachments to spam emails that appeared to contain legitimate files</li> <li>❖ The ransomware encrypted data on the computers, demanding payments of \$300 to \$600 via the digital currency bitcoin to restore access</li> </ul>	<p><b>GLOBAL IMPACT</b></p> <ul style="list-style-type: none"> <li>❖ A cyber security firm said it had seen 2,00,000 cases of the Wanna Cry attack</li> <li>❖ Asian nations also hit hard by the ransomware</li> </ul>

## What are the Legislations to Protect Against Ransomware Attacks in India?

- Ransomware attacks constitute various offences under the [Indian Penal Code 1860](#) and the [Information Technology\(IT\) Act 2000](#).
  - The IT Act has **relevant provisions include: Section 43 and 66 (damage to**

computer/system), **Section 65 (tampering with computer source documents), and Section 66D (cheating by personation)**. Additionally, corporate bodies holding sensitive personal data have an obligation to implement reasonable security practices under the IT Rules.

- The punishment for ransomware attacks under the IT Act ranges from imprisonment for a term of three years to seven years and a fine of up to Rs. 1 crore.
- The **Ransomware Task Force (RTF)** is a specialised unit within **India's National Cyber Security Coordinator (NCSC)** organisation that serves as a central point of contact for victims of ransomware attacks, providing assistance with investigation, recovery, and prevention efforts.
- **Cybersecurity Framework for the Indian Banking Sector, 2018**, issued by the **RBI** provides specific guidelines for banks and financial institutions to protect against cyber threats, including ransomware attacks.
  - It mandates banks to implement robust cybersecurity measures, such as multi-factor authentication, encryption, and regular security audits.

# CYBER SECURITY

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

## CYBER SECURITY ATTACKS

**'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.

### Recent Major Cyber Attacks

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

### 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)

### 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

**Way Forward**

- **Cybersecurity Enhancements:** Banks and technology service providers must implement robust cybersecurity measures, including **endpoint protection, network security, data backup, and employee training.**
  - Improved threat detection and prevention have led to an 11.5% decline in ransomware infections between 2022 and 2023.
  - Establish a centralised platform for sharing **threat intelligence among banks and financial institutions.**
- **Data Backup and Recovery:** Implement robust data backup and recovery procedures, including offline backups. Develop comprehensive business continuity plans to ensure minimal disruption in case of a cyberattack.
- **Enhanced Security Standards:** Conduct rigorous security assessments of third-party vendors and partners. Improve incident response capabilities to minimize the impact of cyberattacks.
  - Obtain relevant **cybersecurity certifications** to demonstrate commitment to security.

**Drishti Mains Question:**

**Q.** Analyze the effects of the ransomware attack on the banking ecosystem and what measures can organisations implement to mitigate these risks?

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

### **Prelims:**

**Q.** The terms 'WannaCry, Petya and EternalBlue' sometimes mentioned in the news recently are related to (2018)

- (a) Exoplanets
- (b) Cryptocurrency
- (c) Cyber attacks
- (d) Mini satellites

**Ans: (c)**

**Q.** 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)

Q. Discuss the potential threats of Cyber-attack and the security framework to prevent it. (2016)

