सत्यमेव जयते
MAHARASHTRA GOVERNMENT
ADDITIONAL DIRECTOR GENARAL OF POLICE MAHARASHTRA
CYBER, WORLD TRADE CENTER, CUFFE PARED-400005
Email: sp.cbr-mah@gov.in

Cyber Threat Landscape – Telecommunication Sector

The Maharashtra Computer Emergency Response Team (MHCERT) has prepared a comprehensive sectorial report on the telecommunication sector. This advisory outline the prevalent threats, key risks, and strategic recommendations to safeguard digital infrastructure within India's telecom networks.

Key Highlights of the Advisory:

- **Targeted Sector:** Telecommunication organizations, including mobile network operators (Reliance Jio, Bharti Airtel, Vodafone Idea, BSNL & MTNL) and telecom infrastructure companies.
- **Observed Threats:**
  - **Data Breaches (40%):** Massive exposure of customer data, including a January 2024 incident affecting 750 million Indian citizens with 1.8TB of compromised data being sold for $3,000.
  - **Nation-State APT Activities:** Groups like APT41 (China), LockBit Group, and Lazarus Group (North Korea) conducting espionage and sabotage against Indian telecom networks.
  - **Ransomware Attacks (20%):** Major telecom operators facing encryption and extortion attempts disrupting critical infrastructure.
  - **SIM Swap Fraud (25%):** Targeting high-net-worth individuals by compromising their mobile numbers to bypass two-factor authentication security.
  - **Call Swapping Scams (15%):** Attackers tricking telecom providers to switch victims' numbers to new SIMs.
- **Impact of Attacks:**
  - **Identity Theft:** Widespread exposure of personal identifiable information including names, phone numbers, addresses, and Aadhaar details.
  - **Financial Losses:** Through unauthorized banking transactions and fraud enabled by SIM swapping.
  - **Service Disruptions:** Affecting critical communications infrastructure supporting emergency services.
  - **National Security Concerns:** Compromise of telecom networks supporting defence and intelligence operations.

- **Recent Incidents:**
  - Major data breach in January 2024 exposing approximately 1.8TB of telecom user data, affecting 85% of India's population.
  - Multiple SIM swapping attacks targeting business executives and high-value individuals.
  - 12 major cyberattacks on telecom sector in 2024, contributing to India ranking as the second most targeted nation globally.
  - Historical incidents including the 2018 Airtel data breach affecting 300 million customers.
- **Mitigation Strategies:**
  - **Enhanced Network Security:** Implement IDS/IPS, SIEM, and DDoS mitigation tools for real-time threat monitoring.
  - **Data Encryption & Privacy:** Ensure end-to-end encryption, data localization, and multi-factor authentication.
  - **Secure Supply Chain:** Conduct regular security audits of vendors, especially for 5G equipment.
  - **Zero Trust Architecture:** Adopt strict access controls to protect sensitive systems and monitor for insider threats.
  - **Employee Training:** Regular cybersecurity awareness programs focusing on phishing detection and secure data handling.
  - **Incident Response & Vulnerability Management:** Maintain comprehensive incident response plans and regular security assessments.
  - **5G Security:** Implement specific security protocols for emerging 5G infrastructure to address new attack surfaces.
  - **Regulatory Compliance:** Align with Telecom Cybersecurity Framework and the Digital Personal Data Protection Act requirements.

THREAT INTELLIGENCE REPORT

TELECOMMUNICATIONS SECTOR

CERTMH_CTI_2025_09

Table of Contents

Executive Summary

The **Indian telecommunication sector**, a critical pillar of the country's digital economy, has witnessed a significant rise in cyber threats since 2020. With the rapid **expansion of 5G networks, IoT adoption, and cloud-based telecom services,** cyber adversaries, including nation-state actors, cybercriminals, and hacktivists, have increasingly targeted India's telecom infrastructure.

Key Threats to Indian Telecom (2019–Present):

- **Nation-State Attacks**: Adversary groups linked to China (APT41, Mustang Panda), Pakistan (Transparent Tribe), and North Korea (Lazarus Group) have engaged in espionage, data theft, and cyber sabotage against Indian telecom networks.
- **Rise of Cybercrime & Fraud:** The surge in SIM swap frauds, mobile banking scams, and phishing attacks targeting telecom users has led to severe financial losses. Exploitation of SS7 vulnerabilities continues to be a major concern.
- **Ransomware & DDoS Attacks:** Indian telecom operators such as BSNL, Airtel, and Jio have faced ransomware incidents, API vulnerabilities, and large-scale DDoS attacks disrupting nationwide services.
- **Supply Chain Risks & 5G Security Challenges:** The adoption of 5G technology has introduced new attack surfaces, including network slicing exploits and IoT vulnerabilities. Regulatory concerns over Chinese telecom equipment vendors (Huawei, ZTE) have further complicated India's security posture.

To counter these threats, **Indian telecom regulators** such as **Telecom Regulatory Authority of India (TRAI), Department of Telecommuniations (DoT), Computer Emergency Response Team - India (CERT-In), and National Critical Information Infrastructure Protection Centre (NCIIPC)** have introduced stringent cybersecurity guidelines, increased collaboration with intelligence agencies, and promoted indigenous security solutions. However, the evolving cyber threat landscape demands continuous monitoring, real-time threat intelligence, and proactive security measures to protect India's telecom ecosystem from future cyber risks.

Industry Overview

The **Indian telecommunication sector** is a **backbone of national security, economic growth, and digital transformation**. With over **1.2 billion mobile subscribers (as of 2024)** and a **rapidly growing 5G infrastructure**, the sector is both a vital enabler of India's digital economy and a prime target for cyber threats.

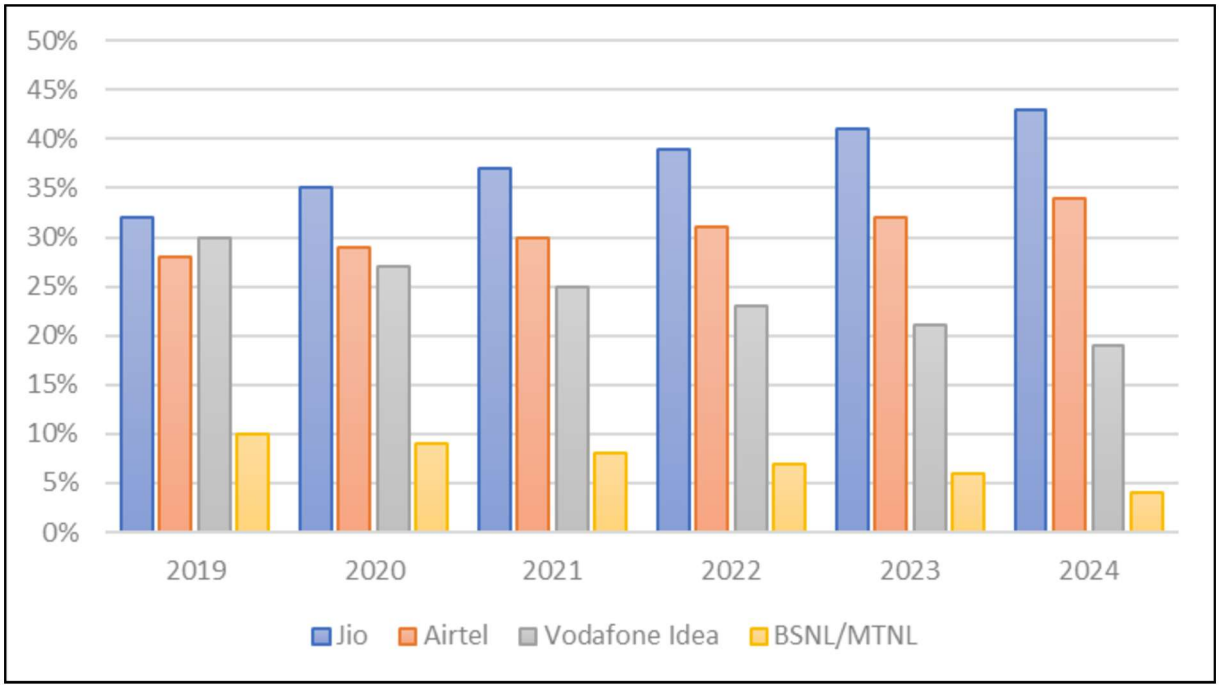
Key Telecom Operators in India (2019 - Present)

TELECOM OPERATOR	MARKET SHARE (%)	SUBSCRIBER BASE (MILLIONS)	GROWTH (2019 - 2024)
Reliance Jio	38.3%	450+	355M (2019) → 510M+ (2024) ~44%
Bharti Airtel	32.2%	390+	330M (2019) → 410M (2024) ~24%
Vodafone Idea (Vi)	18.8%	220+	300M (2019) → 310–320M (2024) ~3-7%
BSNL & MTNL	9.2%	100+	105M (2019) → 140–146M (2024) ~33-39%

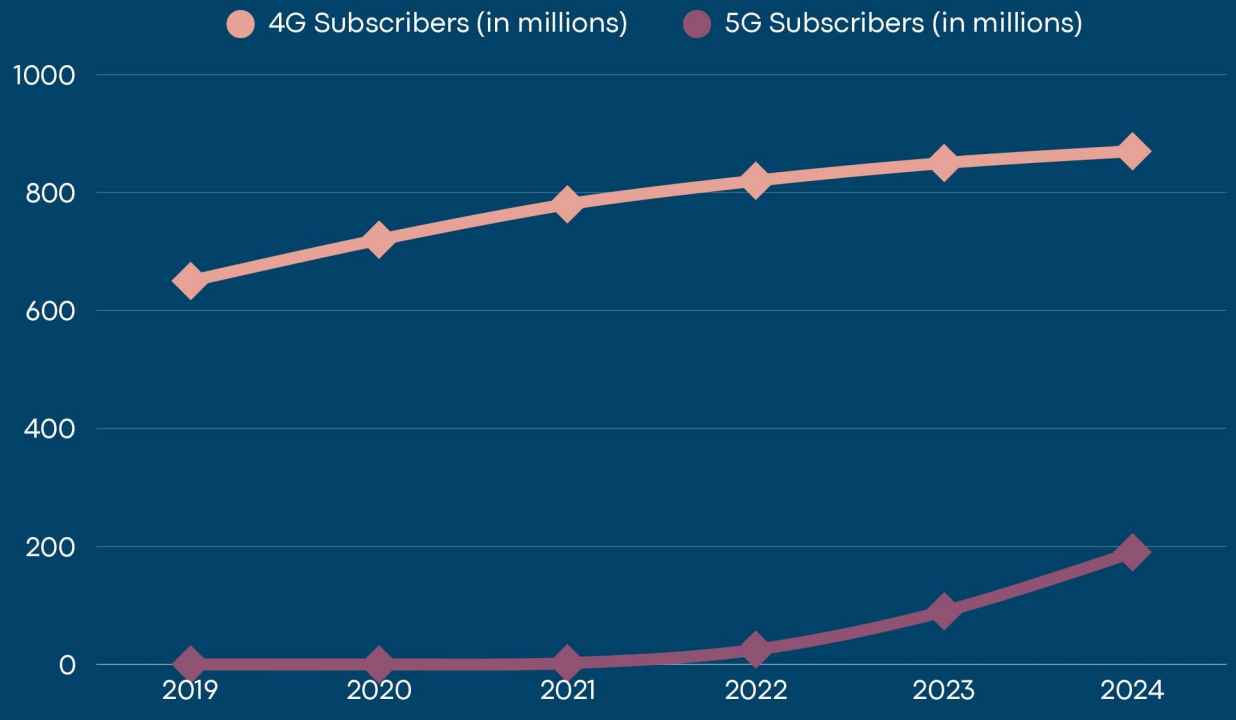
Note:

- Reliance Jio leads the market with aggressive 5G deployment & cloud adoption.
- Airtel has focused on enterprise security solutions and cloud-based telecom networks.
- Vodafone Idea struggles with financial constraints, impacting its cybersecurity budget.
- BSNL & MTNL, being state-owned, face persistent cyber threats due to outdated infrastructure.

Market Share at a Glance



Subscribers at a Glance



India's Critical Infrastructure

Telecom Sector's Role

Contribution to National Security & Economy

- **Economic Impact:** The Indian telecom industry contributes ~6.5% to the national GDP (~USD 170 billion market size in 2023).
- **Employment & Digital Growth:** The sector directly employs ~4 million people and indirectly supports ~10 million jobs.
- **Digital India & Financial Inclusion:** Over 80% of financial transactions in India occur via mobile networks, making telecom security essential for UPI, digital banking, and fintech ecosystems.
- **Government Dependence on Secure Communication:**
  - Defense & Intelligence agencies rely on secure telecom networks for operations.
  - National security concerns arise due to potential espionage by foreign adversaries targeting telecom networks.
  - Cybersecurity incidents affecting telecom can impact emergency services (112 helpline, disaster response, etc.).

The telecom sector is a key pillar of India's economy, contributing ~6.5% to the GDP with a market size of ~$170 billion (2023). It enables **Digital India, UPI payments, fintech, and e-governance**, connecting over 1.2 billion subscribers. The industry directly employs ~4 million people and supports ~10 million jobs, driving economic and technological progress. Telecom networks are critical for national security, supporting defense, intelligence, and emergency services. With 5G expansion, the sector is evolving rapidly but faces cybersecurity threats, including espionage, supply chain risks, and data breaches.

Regulatory & Policy Framework

Governing Indian Telecom Security

The **Indian government** has implemented **strict cybersecurity policies** to protect telecom infrastructure.

Key Regulatory Authorities

Their Role in Cybersecurity

REGULATORY BODY	ROLE IN TELECOM SECURITY
Department of Telecommunications (DoT)	Driving India's telecom growth through policy, licensing, spectrum management, regulation, innovation, and strategic investments.
Telecom Regulatory Authority of India (TRAI)	TRAI ensures fair, competitive, and consumer-centric telecom growth through regulation, policy, and industry oversight.
Computer Emergency Response Team – India (CERT- In)	Swift incident response, threat prevention, forensics, security audits, training, expert guidance, and intel sharing.
National Critical Information Infrastructure Protection Centre (NCIIPC)	NCIIPC safeguards CII through threat defense, risk assessment, proactive security, collaboration, and awareness.

Recent Cybersecurity Directives

(2019 - 2024)

01 2019: DoT

Telecom Security Assurance Requirements (TSAR) enforce security measures like encryption, secure equipment, and audits to protect against cyber threats such as DDoS and SIM swap fraud.

02 2021: TRAI

TRAI's **data localization** mandate secures telecom data within India, strengthening privacy, national security, and regulatory control while boosting the digital economy.

03 2022: CERT-In

CERT-In mandates telecom firms to **report cyber incidents within 6 hours,** ensuring swift response, risk mitigation, and national cybersecurity resilience.

04 2023: DoT

The DoT's 5G Security Guidelines address supply chain risks, specifically targeting threats from Chinese vendors, ensuring secure, reliable 5G infrastructure for India's telecom sector.

05 2024: DPDP Act

India's **Digital Personal Data Protection (DPDP) Act** imposes stringent penalties for telecom data breaches, ensuring robust data privacy and accountability in the telecom sector.

Threat Landscape

Indian Telecom Sector

The Indian telecom sector has become a **high-value target** for cyber adversaries, ranging from **nation-state hackers and cybercriminal groups to hacktivists and insiders.** With over **1.2 billion mobile users** and a growing **5G adoption rate (projected to reach 350 million users by 2025)**, telecom networks serve as the backbone for **critical national communications, banking transactions, and emergency services.**

Since **2020**, Indian telecom operators like **Jio, Airtel, and BSNL** have faced **persistent cyberattacks**, including **espionage-driven APT intrusions, large-scale DDoS attacks, ransomware incidents, and SIM swap frauds.** This section provides a **deep dive into the adversary landscape and the most exploited attack vectors** in the Indian telecom ecosystem.

Cyber Attacks

Indian Telecom Sector (2024)

January 2024:
A significant data breach occurred, involving approximately 1.8 terabytes of data (estimated 750 million records) from major Indian telecom providers. This breach impacted about 85% of the Indian population. The exposed data included sensitive customer details such as names, phone numbers, addresses, and Aadhaar information. Threat actors allegedly attempted to sell the stolen records on underground forums, raising serious concerns about national security and data privacy.

Throughout 2024:
The telecommunications sector experienced 12 major cyberattacks, contributing to India ranking as the second most targeted nation globally, with a total of 95 entities across various sectors affected by data theft. Several of these attacks were attributed to advanced persistent threat (APT) groups, likely backed by nation-states, aiming to compromise critical infrastructure. The breaches led to widespread disruptions, raising alarms about the need for stronger cybersecurity frameworks and regulatory measures.

Types of Cyber Attacks

(2019 - Present)

SIM Card Swapping (25%)

- Attackers use social engineering to convince telecom providers to switch a victim's phone number to a new SIM card, allowing them to intercept messages, calls, and two-factor authentication codes.

Incidents

- SIM swapping enables identity theft and financial fraud by convincing telecom providers to switch numbers. Attackers intercept two-factor authentication codes, gaining access to accounts and stealing sensitive information or funds.

Call Swapping Scam (15%)

- The call swapping scam involves attackers tricking telecom providers to switch a victim's number to a new SIM, giving them control to intercept calls and messages.

Incidents

- In 2020, a high-profile business executive in India fell victim to a call swapping scam, leading to unauthorized access to his bank accounts, highlighting telecom vulnerabilities in number transfer protocols.

Data Breaches (40%)

- Unauthorized access to telecom company databases, leading to the exposure of sensitive customer data.

Incidents

- In 2024, a major breach exposed 750 million records of Indian telecom users, affecting 85% of the population, including sensitive details like phone numbers, addresses, and Aadhaar information.

Ransomware Attacks (20%)

- Malicious software that encrypts telecom data, demanding payment (ransom) for its restoration.

Incidents

- Telecom companies have increasingly been targeted by ransomware groups, impacting critical infrastructure and causing disruptions.

Threat Actors

(2019 - Present)

Sodinokibi

Tactical Intelligence

- Bitcoin: 3AXsdbxDtWd8BKw2tfZxH1nb3rXLKFFxXY
- Operations (Onion Domains):
  - dnpscnbaix6nkwvystl3yxglz.onion
  - aplebzu47wgazapdqks6vrcv6zcnjppkbxbr6wketf56nf6aq2nmyoyd.onion
  - 7nteicqrou3t75tpcc5532cztc46qyd.onion
  - dnpscnbaix6nkwvystl3yxglz7nteicqrou3t75tpcc5532cztc46qyd.onion

Strategic Intelligence

- Specialization: Ransomware
- Origin: Unknown
- Presence in Dark Web & Cybercrime Forums:
  - Forums: XSS, Exploit.in, RAMP4U
- Known Affiliations: Engages in underground ransomware operations

Operational Intelligence

- Tools
  - Rclone
  - ConnectWise
  - Mimikatz
  - Nltest
  - KPOT
  - Qakbot / Qbot / QuackBot / Pinkslipbot
  - Sodinokibi / REvil
  - Cobalt Strike
  - AnyDesk

Technical Intelligence

- Known CVEs Exploited
  - CVE-2019-11510 (Pulse Secure VPN – Arbitrary file reading)
  - CVE-2019-11507 (Exploitation in Pulse Secure VPN)
  - CVE-2021-27065 (Exchange Server Remote Code Execution)
  - CVE-2021-26855 (Microsoft Exchange SSRF vulnerability)
  - CVE-2021-30119 (Potential exploitation in web applications)
  - CVE-2021-26858 (Exchange Server Post-auth Arbitrary File Write)

LAZARUS GROUP

Tactical Intelligence

- Cryptocurrency Wallets:
  - Bitcoin: 1Gf8U7UQEJvMXW5k3jtgFATWUmQXVyHkJt
  - Bitcoin: 1MQC6C4FVX8RhmWESWsazEb5dyDBhxH9he
  - Bitcoin: 1DjyE7WUCz9DLabw5EWAuJVpUzXfN4evta
  - Ethereum: 0x460ab1c34e4388704c5e56e18D904Ed117D077CC
- Telegram Channel: LAZARUS GROUP

Strategic Intelligence

- Specialization: Cyber Crime
- Origin: North Korea
- Known Affiliation: Lazarus Group (North Korean state-sponsored hacker group)
- Operations: Known for a variety of cybercriminal activities, including ransomware, espionage, and financial theft.

Operational Intelligence

- Tools
  - ValeforBeta
  - DAVESHELL
  - HARDRAIN
  - NukeSped.AB
  - VEILEDSIGNAL
  - SLICKSHOES
  - TxRLoader / TAXHAUL
  - Hermes
  - Fimlis.B
  - TAINTEDSCRIBE

Technical Intelligence

- Known CVEs Exploited:
  - CVE-2023-29059
  - CVE-2021-21551
  - CVE-2017-0199
  - CVE-2016-4117
  - CVE-2016-1019

LockBit Group

Tactical Intelligence

- Contact Details:
  - Jabber: 598954663666452@exploit.im
  - Jabber: 365473292355268@thesecure.biz
  - Tox: 3085B89A0C515D2FB124D645906F5D3DA5CB97CEBEA975959AE4F95302A04E1D709C3C4AE9B7
  - Tox: 3085B89A0C515D2FB124D645906F5D3DA5CB97CEBEA975959AE4F95302A04E1D14E41080A105
- Operations (Onion Domains):
  - lockbitapt5x4zkjbcqmz6frdhecqqgadevyiwqxukksspnlidyvd7qd.onion
  - lockbitaptq7ephv2oigdncfhtwhpqgwmqojnxqdyhprxxfpcllqdxad.onion
  - lockbitaptstzf3er2lz6ku3xuifafq2yh5lmiqj5ncur6rtlmkteiqd.onion
  - lockbitaptc2iq4atewz2ise62q63wfktyrl4qtwuk5qax262kgtzjqd.onion
  - yq43odyrmzqvyezdindg2tokgogf3pn6bcdtvgczpz5a74tdxjbtk2yd.onion
  - lockbitapt2yfbt7lchxejug47kmqvqqxvvjpqkmevv4l3azl3gy6pyd.onion
  - lockbitapt34kvrip6xojylohhxrwsvpzdffgs5z4pbbsywnzsbdguqd.onion
  - oyarbnujct53bizjguvolxou3rmuda2vr72osyexngbdkhqebwrzsnad.onion
  - lockbitapt6vx57t3eeqjofwgcglmutr3a35nygvokja5uuccip4ykyd.onion

Strategic Intelligence

- Specialization: Ransomware
- Origin: Unknown
- Known Affiliation: LockBit (Ransomware-as-a-Service operator)
- Operations: Multiple onion domains for data leaks and negotiations

Operational Intelligence

- Data Leaks (Affected Entities):
  - Apollo Scientific Leak-filetree
  - mangiainc.com
  - gruppomercurio.com
  - tsmc.com

APT 41

Tactical Intelligence

- Tools
  - Outloader
  - pwdump
  - XMRig (Cryptomining tool)
  - POISONPLUG / ShadowPad (Remote access trojan)
  - Ping
  - HIGHNOON (Backdoor malware)
  - BLACKCOFFEE (Persistence tool)
  - Encryptor RaaS (Ransomware-as-a-Service tool)
  - Symatic loader
  - CroxLoader (Loader for malicious payloads)

Strategic Intelligence

- Specialization: Espionage
- Aliases: Wicked Panda
- Origin: China
- Known Affiliation: Chinese state-sponsored threat actor group
- Primary Objective: Cyber espionage, targeting sensitive data and information from various sectors.

Operational Intelligence

- Campaigns:
  - APT 41 Dust: Targeted sectors such as shipping, logistics, and media for information gathering purposes.

Technical Intelligence

- Known CVEs Exploited:
  - CVE-2012-0158
  - CVE-2021-34527
  - CVE-2020-8193
  - CVE-2019-1652
  - CVE-2019-1653
  - CVE-2019-19781
  - CVE-2021-26855
  - CVE-2021-44228
  - CVE-2017-0199
  - CVE-2019-16278

Indian Telecom Data Breach

(2024)

A significant cybersecurity breach has been uncovered, exposing the personal information of **750 million individuals** in India. The breach involves sensitive data, including **names, mobile numbers, addresses,** and **Aadhaar information.** This massive dataset, totaling **1.8 terabytes,** is being sold by **CyboDevil** and **UNIT8200**, two threat actor groups with a history of cybercriminal activities. The breach affects **85%** of India's population and poses severe risks to individuals and organizations.

Impact:

The breach presents several risks, including:

- **Identity Theft:** Exploitation of personal data for fraudulent activities.
- **Financial Losses:** Potential for cyberattacks targeting financial accounts.
- **Increased Cyberattack Susceptibility:** Enhanced vulnerability to phishing and scams targeting individuals.

Key Details:

- Detected by: CloudSEK's XVigil AI platform on January 23, 2024.
- Cyber Attackers: CyboDevil and UNIT8200 (CYBOCREW group members).
- Dataset Size: 1.8TB (compressed to 600GB).
- Price Demanded: $3,000 for the complete dataset.
- Affected Telecom Providers: All major telecom operators in India.
- Exposed Information: Personal Identifiable Information (PII) – names, mobile numbers, addresses, Aadhaar information.
- Threat Actor Activity:
  - Previous incidents included access to real-time Indian phone number KYC details.
  - Sale of API access to the Indian vehicle database.
- Source of Data: The threat actors claim the data was obtained through undisclosed operations within law enforcement channels, not via a traditional data breach.
- Verification Status: Analysis of a sample dataset indicates the information pertains to subscribers of all major telecom providers in India, with Aadhaar numbers confirmed as valid.
- Government Response: The Department of Telecom (DoT) has taken action and instructed telecom operators to conduct security audits of their systems.

SIM Swapping Fraud

(Multiple Incidents)

SIM card swapping attacks have emerged as a prominent cybersecurity threat in India, with several high-profile incidents over the years. Cybercriminals use **social engineering techniques** to convince telecom providers to swap a victim's SIM card to a new device, thereby gaining control of their phone number. Once the attackers control the number, they can bypass **two-factor authentication (2FA),** allowing them to access **banking accounts, social media profiles,** and other sensitive information.

Impact:
The risks associated with SIM card swapping include:

- **Financial Losses:** Hackers can access banking apps, transfer funds, or perform fraudulent transactions using 2FA bypass.
- **Identity Theft:** Personal data from phone contacts, messages, and accounts can be stolen and misused.
- **Increased Vulnerability:** Once the victim's phone number is compromised, other personal accounts (e.g., email, social media) are also at risk.

Key Details:

- Attack Type: SIM card swapping (also known as SIM swap fraud).
- Targeted Entities: Telecom providers and individual victims, particularly high-net-worth individuals.
- Method: Hackers impersonate the victim, convince telecom operators to switch the victim's SIM to a new one, and gain control of the phone number.
- Exploited Vulnerability: Dependency on SMS-based 2FA for authentication.
- Notable Incidents: Attacks on businessmen, SBI customers, and high-net-worth individuals.
- Attack Execution: Fraudsters often use phishing, data leaks, or social engineering to gather personal details before requesting a SIM swap.
- Telecom Provider Response: Regulatory bodies like TRAI and CERT-In have issued advisories, urging telecom operators to strengthen KYC verification for SIM replacement requests.

Airtel Data Breach

(Alleged - 2018)

In 2018, a significant data breach occurred involving **Airtel**, one of India's leading telecommunications companies. This breach exposed the **personal data** of **over 300 million customers,** including sensitive details such as **names, phone numbers, and addresses.** The breach was discovered after a misconfigured database was found publicly accessible on the internet, allowing unauthorized access to this vast amount of customer information.

Impact:

- **Identity Theft:** Exposure of personal information increases the risk of fraud and identity theft.
- **Phishing and Spam:** Attackers may use the exposed data to conduct phishing or spam campaigns.
- **Financial Losses:** Customers may experience financial losses if their personal data is exploited for fraudulent purposes.

Key Details:

- Breach Detected: 2018.
- Exposed Data: Personal details of 300 million customers, including names, phone numbers, and addresses.
- Root Cause: Misconfigured server that was left unsecured and publicly accessible.
- Potential Impact: Unauthorized access to sensitive customer data, potential misuse for fraud, and data resale.
- Breach Discovery: The breach was uncovered by Security researchers who discovered that the database was unprotected and indexed by search engines, making it easily discoverable.
- Response: Airtel immediately took down the misconfigured server and initiated a security audit. However, the company did not initially disclose the breach to the public, which led to criticism from data privacy advocates.

Conclusion

Since 2019, the Indian Telecom Sector has become a cornerstone of economic growth, **contributing ~6.5% to GDP** and supporting over **1.2 billion subscribers.** With **Reliance Jio** leading the charge in **5G adoption** and digital services, telecom has powered **Digital India, financial inclusion, and e-governance.** The sector has also created millions of jobs and contributed significantly to the **digital economy.**

However, the rapid expansion of **5G and IoT** introduces new **cybersecurity risks,** prompting stronger regulatory frameworks from **DoT, TRAI, and CERT-In.** Despite challenges, the telecom sector remains poised for continued growth, leveraging **cutting-edge technologies** to drive **smart cities, autonomous vehicles,** and more. With ongoing innovation and resilience, India's telecom industry is on track to shape a **digitally empowered future** on the global stage.

Looking ahead, **5G technology** will be the **game-changer** for India, unlocking new opportunities in industries ranging from healthcare to manufacturing, enabling **hyper-connectivity** and fueling the **next wave of digital transformation.** While challenges like **cybersecurity and regulatory hurdles** persist, the sector's strong foundation and continuous innovation make it well-positioned to maintain its role as a leader in India's economic and technological landscape.

Moreover, the **collaborative efforts** between the **government, telecom operators, and regulatory bodies** will play a pivotal role in ensuring **security, compliance, and sustainable growth** in the sector. As India moves towards a **5G-enabled future,** it must remain vigilant about potential **cyber threats, data privacy concerns, and global competition** to maintain its position as one of the **world's largest and most advanced telecom markets.**

In conclusion, the journey of India's telecom sector from 2019 to present is a story of unprecedented **growth, innovation, and resilience—one that continues to lay the groundwork for a connected, digitally-empowered** India in the years to come.

Recommendations

- **Enhanced Network Security:** Implement IDS/IPS, SIEM, and DDoS mitigation tools for real-time threat monitoring and incident detection.
- **Data Encryption & Privacy:** Ensure end-to-end encryption, data localization, and multi-factor authentication (MFA) for sensitive data and communications.
- **Secure Supply Chain:** Conduct regular security audits and penetration testing for third-party vendors to avoid supply chain vulnerabilities, especially with foreign equipment.
- **Access Controls & Insider Threats:** Adopt Zero Trust Architecture (ZTA), enforce role-based access, and monitor for insider threats to protect sensitive systems.
- **Employee Training & Awareness:** Regularly train staff on cybersecurity best practices, phishing detection, and secure data handling.
- **Disaster Recovery & Business Continuity:** Develop disaster recovery plans with data backups and failover systems to ensure service continuity during cyber incidents.
- **Incident Response & Vulnerability Management:** Maintain an incident response plan, patch vulnerabilities, and conduct regular security assessments.
- **Threat Intelligence Sharing:** Join industry-specific platforms and collaborate with bodies like CERT-In for real-time threat intelligence and proactive defense.
- **5G Security:** Implement 5G-specific security protocols, secure RAN, core networks, and IoT devices to address emerging threats.
- **Regulatory Compliance:** Align with Telecom Cybersecurity Framework and data protection laws to meet national and international security standards.

References

Indian Department of Telecommunication

- https://dot.gov.in/circulars/cyber-security-best-practices-reg

Telecom Regulatory Authority of India

- https://www.trai.gov.in/sites/default/files/2024-10/Annaul_Report_23022023_0_0.pdf

India Brand Equity Foundation (IBEF)

- https://www.ibef.org/industry/telecommunications

Computer Emergency Response Team - India

- https://www.cert-in.org.in/PDF/guidelinesgovtentities.pdf

News Agencies:

The Hindu:

- https://www.thehindu.com/sci-tech/technology/internet/hacker-claims-to-have-accessed-airtels-customer-database-company-denies-data-breach/article68370519.ece#:~:text=Earlier%20in%202021%2C%20a%20cybersecurity,that%20any%20breach%20had%20occurred

The Times of India

- https://timesofindia.indiatimes.com/technology/tech-news/reliance-jio-has-a-cyber-fraud-warning-for-its-customers-what-it-is-and-how-to-stay-safe/articleshow/112737224.cms