

Redefining cybercrime investigations: A holistic framework for law enforcement in the digital age

February 2025





Contents

About Grant Thornton Bharat LLP	4
About Future Crime Research Foundation (FCRF)	5
Introduction	6
Key trends	6
– Current cybercrime trends	6
– Current investigation support ecosystem	7
– Cybercrime investigation lifecycle	7
– New age cybercriminals	8
– Role of police	8
– Increase in cybercrime cases in India	9
– The global reach of cybercrime	10
Investigation framework and traditional approach	11
– Cybercrime management ecosystem	12
– Proposed framework for cybercrime investigations	12
– Traditional investigation approach	14
– Challenges and roadblocks	14
Recommendations for enhancing cybercrime investigations in India	15
– Enhancing investigation capabilities	16
– Strengthening cyber security policies	18
– Raising cyber awareness among citizens	20
Conclusion	21
References:	21
Glossary of key terms	22
Acknowledgements	23

About Grant Thornton Bharat LLP

A member of Grant Thornton International Ltd, Grant Thornton Bharat is a leading professional services firm in the country. A truly Indian Firm with global connections - we work with businesses and governments across industries and sectors, providing assurance, consulting, tax, risk and digital and technology transformation services.

At Grant Thornton, we believe that adequate cyber security is not just about technology but also about people and processes. We work closely with our clients to build a culture of security awareness and resilience, fostering an environment where cyber security is integrated into every aspect of their operations.

Our comprehensive cyber security services are designed to help organisations navigate the complex and ever-evolving threat environment. We offer a range of solutions to prepare, protect, and respond to cyber threats, ensuring your business remains resilient and secure.

Our services include:

- **Cyber security risk and threat assessments:** Identifying and evaluating potential risks to your organisation.
- **Security policy development:** Crafting robust policies to safeguard your digital assets.
- **Technical assessments and third-party assurance:** Ensuring your systems and third-party partners adhere to the highest security standards.
- **Security architecture and technology implementations:** Building and deploying secure frameworks and technologies.
- **Identity and access management:** Controlling access to critical systems and data.
- **Privacy and data protection:** Safeguarding sensitive information and ensuring compliance with data protection regulations.
- **Incident readiness and response:** Providing rapid and effective responses to security breaches.

About Future Crime Research Foundation (FCRF)

The Future Crime Research Foundation (FCRF) is an IIT Kanpur AIIDE-CoE incubated non-profit organisation dedicated to cybersecurity research, digital forensics, and capacity building in India. As a leading think tank, FCRF actively collaborates with government bodies, law enforcement agencies, and industry leaders to address the evolving challenges of cybercrime and technology-driven threats.

FCRF has signed Memorandums of Understanding (MoUs) with esteemed institutions, including:

- Dr. Ram Manohar Lohiya National Law University (RMLNLU)
- Bankers Institute of Rural Development (BIRD) Lucknow
- Uttar Pradesh State Institute of Forensic Science (UPSIFS)

FCRF also owns [The420.in](https://www.the420.in), India's largest news platform dedicated to cybercrime, technology, and corruption, with a reach of over a million readers. Through investigative journalism and in-depth analysis, [The420.in](https://www.the420.in) serves as a critical resource for professionals, policymakers, and law enforcement agencies.

As part of its commitment to enhancing cyber awareness, FCRF launched the Cyber Safe Uttar Pradesh campaign, a pioneering initiative aimed at equipping citizens and law enforcement with the knowledge and tools to combat cyber threats. Additionally, FCRF annually organises its flagship event, the FutureCrime Summit, India's largest conference on cybercrime, digital forensics, and technology laws. The summit brings together global experts, policymakers, and industry leaders to discuss emerging cyber threats, investigative strategies, and legal frameworks to build a more cyber-resilient nation.



Introduction

As India witnesses an alarming rise in cybercrime, the conviction rates highlight the challenges faced by the justice system in responding effectively. According to the National Crime Records Bureau (NCRB), between 2020 and 2022, over 167,000 cybercrime cases were registered nationwide, but only 2,706 convictions were secured—a mere 1.6% link.¹

States such as Uttar Pradesh, Karnataka, and Telangana consistently top the charts in cybercrime registrations, but their conviction rates remain low, often between 0% and 2%. For instance, in 2021, Karnataka registered over 8,000 cases but managed only 10 convictions. This gap underscores the urgent need to train police investigators and equip them with advanced cyber investigation tools. Without skilled personnel and modern technology, justice remains out of reach for most victims, emboldening cybercriminals and undermining public trust in law enforcement.

In 2022, India reported 65,893 cybercrime cases, with states like Telangana, Uttar Pradesh, and Karnataka leading in the number of cases registered.² The financial impact is also significant, with substantial amounts reported lost to online fraud and other cybercrimes. Over 31 lakh cybercrime complaints have been reported on the National Cybercrime Reporting Portal (NCRP), and more than 66,000 FIRs have been registered by Law Enforcement Agencies of States/UTs to date. To date, the NCRP has helped save over INR 3,431 crore through the resolution of 9.94 lakh complaints.³

Cybercrime has become a significant threat to individuals, businesses, and governments. Investigations are crucial to safeguarding sensitive information, preventing financial losses, and maintaining national security. However, law enforcement agencies face numerous challenges in combating cybercrime, including outdated laws, lack of international coordination, privacy concerns, and resource constraints.

This paper proposes governance and tactical solutions to address these challenges, emphasising the need for a robust legal framework, advanced investigative tools, and enhanced international cooperation.

Key trends

Current cybercrime trends

In recent years, various forms of cybercrime have significantly risen across India, necessitating targeted strategies and awareness campaigns to combat these threats effectively. Data compiled by the NCRP under the Ministry of Home Affairs (MHA) reveals a significant surge in cybercrime incidents in India over the past four years. Fraudsters have cheated people out of a total of INR 33,165 crore, with INR 22,812 crore lost in 2024 alone. Tier 2 and 3 cities are significant hotspots for these crimes.

According to FCRF's white paper, **'A Deep Dive into Cybercrime Trends Impacting India,'** different regions are experiencing specific types of cybercrimes, highlighting the need for localised approaches. For instance, Rajasthan is grappling with sextortion, OLX fraud, and KYC scams, while Jharkhand faces issues like loan app harassment and matrimonial fraud. Delhi and Bihar deal with fake links, OTP frauds, and social engineering scams.

Emerging cybercrime hotspots such as Chittoor in Andhra Pradesh, Barpeta in Assam, and several areas in Delhi and Gujarat demand proactive measures to curb digital criminal activities. The surge in cybercrime incidents can be attributed to various factors, including low technical barriers to entry, inadequate KYC processes, and the availability of fake resources.

Here are some key emerging trends in cybercrime:

- **Sextortion:** Cybercriminals exploit victims by threatening to release private and sensitive information unless a ransom is paid.
- **Phishing and social engineering:** Deceptive tactics trick individuals into divulging sensitive information, leading to financial loss and identity theft.
- **Online fraud:** Scams such as investment fraud, job scams, and digital shopping fraud are prevalent, causing victims financial and emotional harm.
- **Identity theft:** Personal information is stolen and misused to commit fraud, leading to long-term consequences for individuals.
- **Digital arrests:** Law enforcement agencies increasingly make arrests based on digital evidence, highlighting the importance of advanced investigative tools and techniques.

¹ Press Information Bureau

² National Crime Records Bureau

³ Press Information Bureau

- **Cyberstalking and harassment:** Individuals are targeted and harassed online, leading to psychological trauma and fear.

These trends underscore the need for comprehensive strategies to address cybercrime's evolving nature, including enhanced investigative capabilities, robust legal frameworks, and increased public awareness.

Current investigation support ecosystem

The methods used to investigate cybercrime in India continually evolve to keep pace with the rapidly changing threat landscape. Some of the key components of this ecosystem are:

Digital forensics involves using advanced tools to collect, analyse, and preserve digital evidence from personal devices, online accounts, and networks. This process is crucial for ensuring that digital evidence is admissible in court and can withstand legal scrutiny.

Open-source intelligence (OSINT) involves investigators relying on publicly available information from social media, news websites, and public records to gather intelligence and track cybercriminal activities. However, it is important to note that OSINT sources do not yet have complete legal sanctity in India, which can challenge the admissibility of such evidence in legal proceedings.

Collaboration and information sharing are also vital components of the cybercrime investigation ecosystem. Law enforcement agencies often collaborate with private sector organisations, cybersecurity firms, and international bodies to share information, resources, and best practices. This collaborative approach helps pool expertise and resources, leading to more effective investigations and quicker resolution of cybercrime cases.

Despite these advancements, the ecosystem faces several challenges, including the need for continuous training of law enforcement personnel, the development of standardised protocols for handling digital evidence, and the establishment of legal frameworks that recognise and validate the use of OSINT. Addressing these challenges is essential for building an effective cybercrime investigation ecosystem in India.

Cybercrime investigation lifecycle

Cybercrime investigations can vary widely depending on the nature of the crime and the resources available. Some common styles of investigations in India include:

- 01 **Complaint / First information report (FIR) Registration at Police Stations:** Citizens can file complaints at local police stations, which are then transferred to cyber cells for investigation.

- 02 **Cybercrime police station / Cybercell Investigation:** Specialised cyber cells conduct detailed investigations, using digital forensic tools and techniques to gather evidence.
- 03 **Forensic support:** Forensic labs analyse digital evidence to support cybercrime investigations and ensure its court admissibility.
- 04 **Collaboration with Internet Service Providers and other intermediaries:** Cyber cells request data from ISPs and websites to trace cybercriminal activities and gather evidence.
- 05 **Cross-border collaboration:** Indian investigators collaborate with international agencies to track and apprehend cybercriminals abroad.
- 06 **Chargesheet:** Filed after the completion of the investigation, documenting the evidence and findings to formally accuse the suspect in court.
- 07 **Court process:** Conducting of hearings where digital evidence is examined, and concluding with a verdict based on the findings.
- 08 **Passing the verdict:** The judge or jury reviews digital evidence and delivers a decision of either acquittal (not guilty) or conviction (guilty).

New age cybercriminals

Cybercriminals Individual cybercriminals who deceive citizens and exploit systems for financial gain	Online fraud cartels Organised groups that engage in large-scale online fraud, such as phishing, identity theft, and financial scams	Insiders Employees or contractors who misuse their access to commit cybercrimes
State-sponsored hackers Cybercriminals employed by or supported by governments to conduct espionage or sabotage.	Ransomware operators Cybercriminals who use ransomware to encrypt victims' data and demand payment for decryption keys	Organised crime gangs Sophisticated criminal organisations that engage in large-scale cybercrime operations

Role of police

Police agencies in India play a crucial role in combating cybercrime and ensuring the safety of citizens in the digital age. These agencies are responsible for investigating cybercrimes, gathering evidence, and prosecuting offenders. The process typically involves several key steps:

Reporting and initial response

Cybercrime reporting in India can be categorised into two main channels:

1. Central government platforms - (MHA-Managed) – 1930 (Cybercrime Helpline) & Cybercrime.gov.in
2. State-level mechanism - Local police stations, cybercrime police stations, 112, and state-specific cyber reporting applications

Preliminary investigation:

Once a complaint is received, law enforcement conducts a preliminary investigation to assess the nature and severity of the cybercrime. This involves collecting digital evidence, analysing electronic records, and interviewing relevant individuals to establish the case's credibility and direction.

Cybercrime coordination

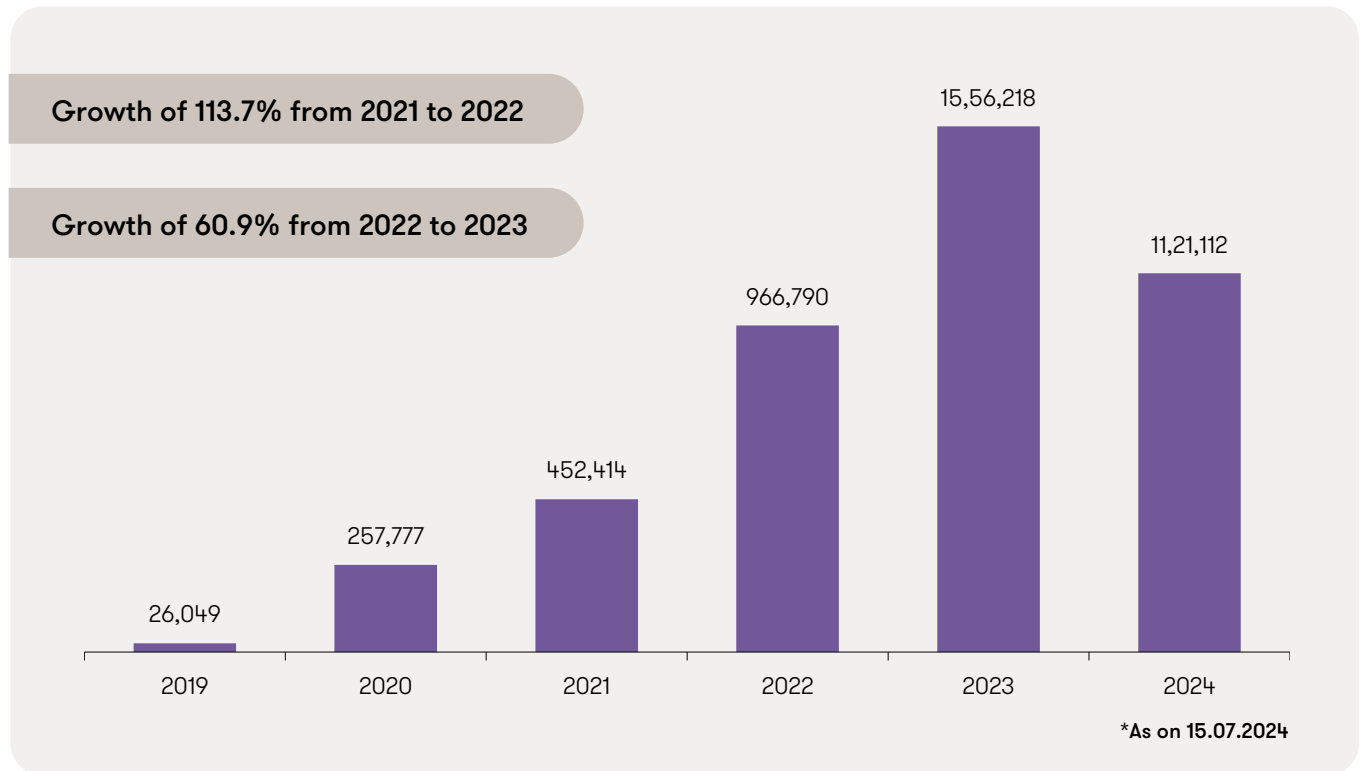
- **Central level coordination – Indian Cyber Crime Coordination Centre (I4C)**

The Indian Cyber Crime Coordination Centre (I4C), under the Ministry of Home Affairs, oversees nationwide efforts to combat cybercrime. It provides policy direction, facilitates intelligence sharing, and supports law enforcement with tools, training, and forensic capabilities. I4C also manages national reporting platforms like 1930 and cybercrime.gov.in, ensuring a coordinated response to cyber threats.

- **State-level coordination – Cybercrime police stations and cybercrime cells**

At the state level, cybercrime investigations are handled by dedicated cybercrime police stations and cybercrime cells. These units operate under state law enforcement agencies, handling cybercrime complaints, conducting investigations, and collaborating with central agencies when necessary. Some states also have dedicated cybercrime reporting apps to streamline complaint registration and case tracking.

Increase in cybercrime cases in India ⁴



⁴ Indian Cyber Crime Coordination Centre

In the last two years, the frequency and severity of cybercrimes have increased significantly. Key statistics include:

- **Financial fraud**

- The National Cyber Crime Reporting Portal has helped resolve 994,000 cybercrime complaints, preventing potential losses exceeding INR 3,431 crore.⁵
- The ‘Cyber Fraud Reporting and Management System’ under the Indian Cyber Crime Coordination Centre (I4C) received approximately 11.28 lakh complaints of cyber fraud from 36 States and Union Territories in 2023. The total financial loss reported through these complaints was about INR 921.59 crores⁶

- **Social media-related fraud**

- The I4C has categorised ‘online and social media-related crime’ as a distinct area of focus, highlighting the rising challenges posed by cybercriminals exploiting these platforms.
- In 2024, India saw a significant rise in online fraud cases, with 17,10,505 complaints registered. The financial losses due to cyber fraud amounted to INR 22,812 crore in 2024.⁷

- **Other specialised cybercrime**

- Experts warn of increased AI-driven cybercrimes in India, as AI tools enable even non-technical criminals to launch sophisticated attacks.⁸
- The Data Security Council of India (DSCI) predicts that by 2025, AI-powered malware and deepfake-based phishing attacks will infiltrate critical infrastructure and personal data, making detection harder.⁹
- The number of digital arrests related to cybercrimes has increased, with over 17,000 WhatsApp accounts connected to digital arrest scams being blocked by the Ministry of Home Affairs.¹⁰

The global reach of cybercrime

Cybercrime knows no national borders, and its impact is felt worldwide. Cybercriminals operate across multiple jurisdictions, making investigations and prosecutions challenging. For instance, the **Equifax data breach in 2017** exposed the personal information of nearly 147 million individuals, highlighting the global nature of cyber threats.¹¹ Similarly, the WannaCry ransomware attack 2017 affected over 200,000 computers across 150 countries, demonstrating the widespread reach of cyber criminals.¹²

- **The AIIMS cyberattack (2022):** A massive ransomware attack which crippled its digital systems and led to a significant data breach. The investigation revealed that the attack originated from China, and five physical servers were infiltrated
- **UPSRTC e-ticketing system hack (2023):** This ransomware attack disrupted services and prompted manual ticketing for over a week. Investigations found that foreign hackers were responsible and demanded a ransom of INR 40 crore in bitcoin.
- **Attempted attack on Maharashtra's Power Grid (2020):** A malware attack caused a major blackout in Mumbai, impacting millions of residents. The investigation confirmed that the malware was introduced by unverified sources, with suspicions pointing towards Chinese hackers
- **Bharat Bill Payment System (BBPS) Fraud (2021):** Cybercriminals targeted the BBPS, a platform for paying utility bills, and siphoned off funds from users' accounts. The investigation found that the attackers used sophisticated phishing techniques to access users' credentials and transfer money to their accounts.
- **Online Banking Fraud (2022):** A series of online banking frauds targeted individuals across India. Cybercriminals use malware to steal login credentials and transfer funds from victims' accounts. The investigation revealed that the attackers were part of an organised crime group operating from multiple countries, including India. The interconnected nature of the digital world means that cybercriminals can operate from anywhere, targeting victims across borders.

⁵ Press Information Bureau

⁶ Cyber Digest by Indian Cyber Crime Coordination Centre

⁷ World Economic Forum

⁸ Ministry of Electronics and Information Technology (MeitY)

⁹ DSCI

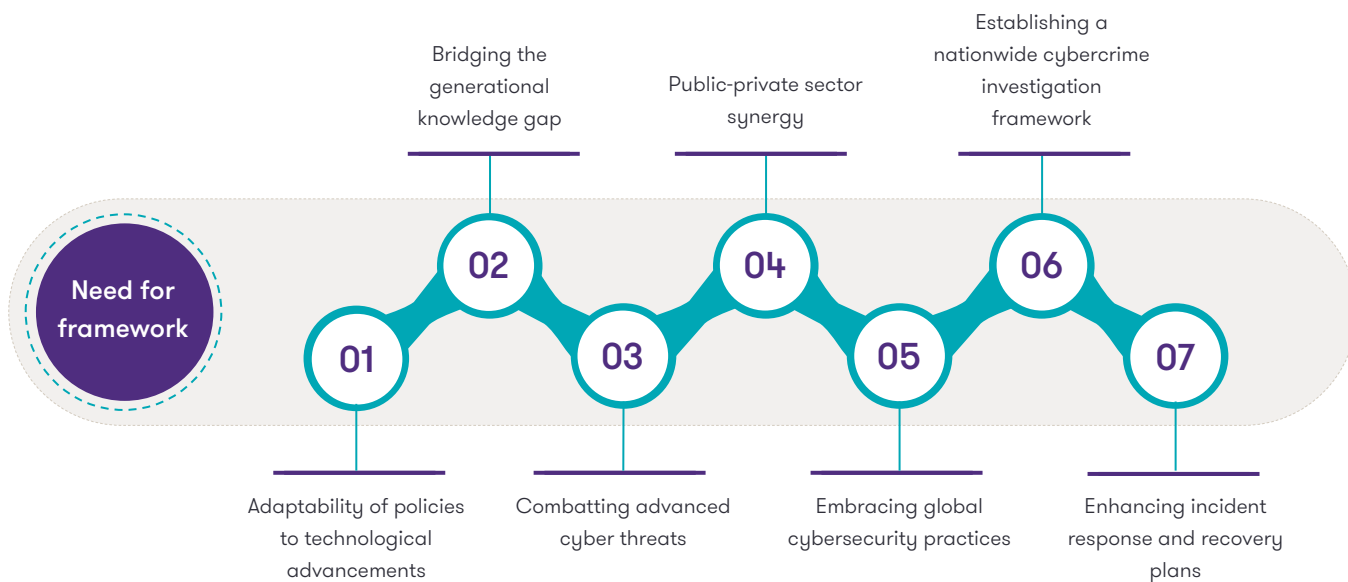
¹⁰ World Economic Forum

¹¹ FTC

¹² Cloudflare

Investigation framework and traditional approach

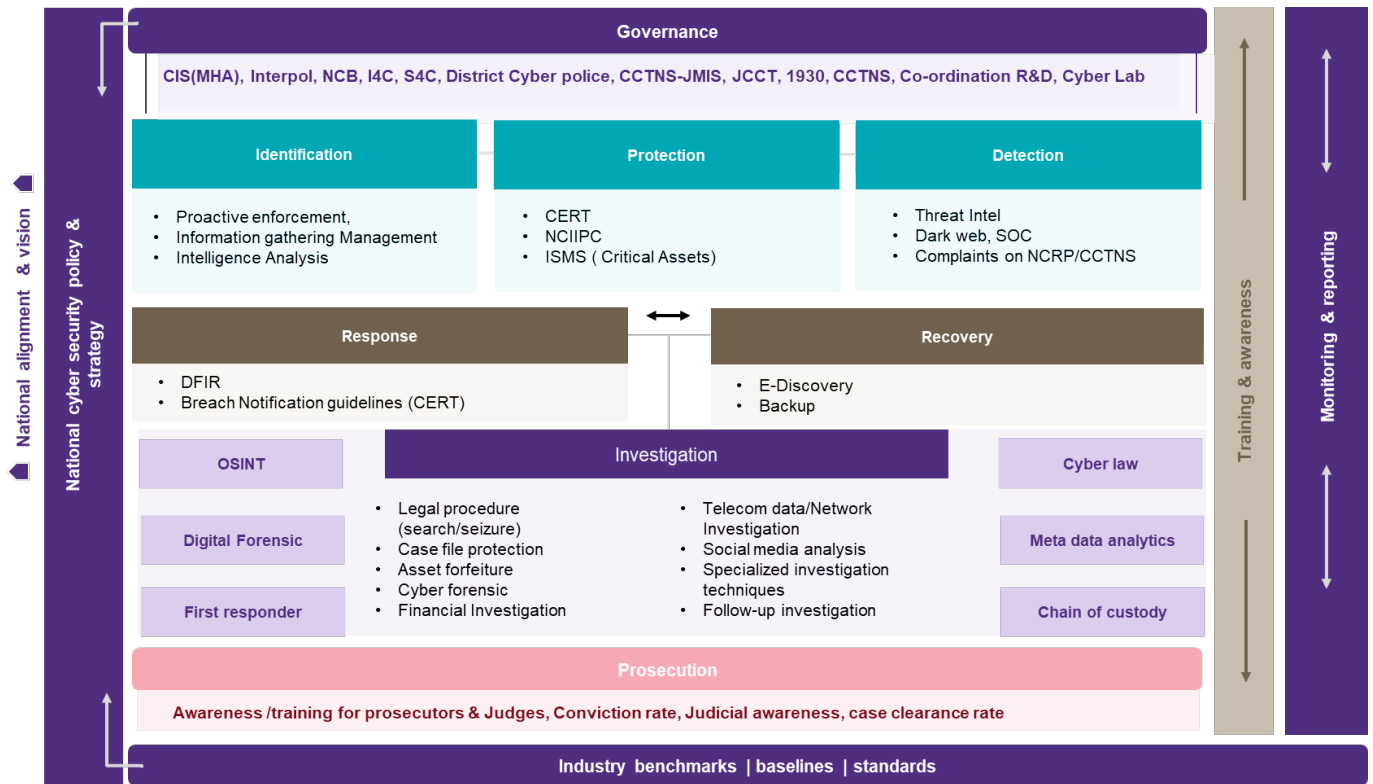
Building on the necessity for an updated cybercrime investigation model in India, the following key aspects must be considered to ensure the framework is comprehensive, proactive, and resilient.




The investigation of cybercrimes in India follows a structured framework designed to ensure systematic and efficient handling of cases. This framework includes various steps and involves multiple agencies working in coordination.



Cybercrime management ecosystem




Proposed framework for cybercrime investigations



Governance

Effective governance is crucial for coordinating efforts across various agencies and ensuring a unified approach to cybercrime investigations. Key entities involved include the Cyber and Information Security (CIS) division of the Ministry of Home Affairs (MHA), Interpol, the Narcotics Control Bureau (NCB), the Indian Cyber Crime Coordination Centre (I4C), and the State Cyber Crime Coordination Centre (S4C). District Cyber Police, the Crime and Criminal Tracking Network and Systems (CCTNS), and the Joint Cyber Crime Coordination Team (JCCT) also play significant roles. The governance framework emphasises coordination in research and development, the transfer of cyber lab capabilities to specialised units, and helplines like 1930 for reporting cybercrimes.



Identification

The identification phase focuses on proactive enforcement and the systematic gathering and management of information. Intelligence analysis is critical, enabling authorities to identify potential threats and vulnerabilities. This phase involves collecting data from various sources, including public reports and intelligence networks, to understand the cyber threat landscape comprehensively.



Protection

Protection measures are designed to safeguard critical assets and infrastructure. The Computer Emergency Response Team (CERT) and the National Critical Information Infrastructure Protection Centre (NCIIPC) are key organisations. Implementing Information Security Management Systems (ISMS) for critical assets ensures robust security protocols are in place to prevent unauthorised access and mitigate potential threats.



Detection

Detection involves monitoring and identifying cyber threats through various means. Threat intelligence, dark web monitoring, and Security Operations Centers (SOC) are pivotal in this phase. Complaints received through platforms like the National Cyber Crime Reporting Portal (NCRP) and CCTNS are also crucial for promptly detecting and responding to cyber incidents.



Response

The response phase includes Digital Forensics and Incident Response (DFIR) to address and mitigate the impact of cyber incidents. CERT's breach notification guidelines provide a framework for informing affected parties and taking necessary actions to contain and remediate breaches.



Recovery

Recovery focuses on restoring affected systems and data. E-Discovery and backup solutions are essential components, ensuring that critical data can be recovered and normal operations can resume swiftly after an incident.



Investigation

The investigation phase involves a comprehensive approach to uncovering the details of cybercrimes. Digital forensics is used to collect, preserve, and analyse digital evidence. Open-Source Intelligence (OSINT) helps track cybercriminal activities through publicly available information. Coordination with Internet Service Providers (ISPs) and technology companies is vital for obtaining relevant data. Other techniques include metadata analytics, legal procedures for search and seizure, case file protection, asset forfeiture, financial investigations, telecom and network investigations, social media analysis, and specialised investigation techniques.



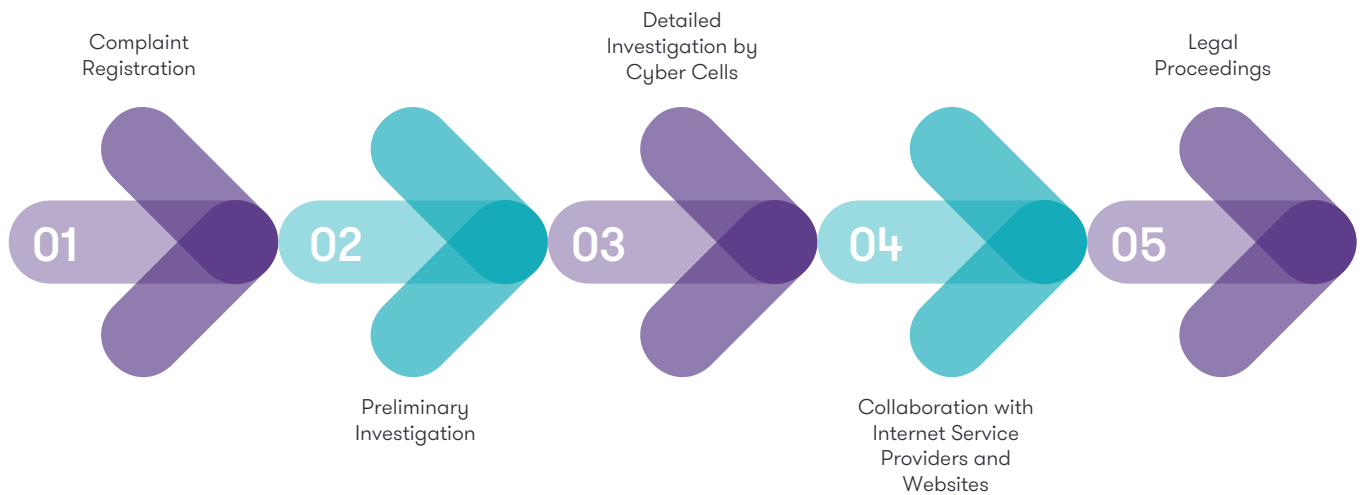
Prosecution

Once sufficient evidence is gathered, law enforcement authorities proceed with legal proceedings against the cybercriminals. This phase ensures that perpetrators are held accountable and serves as a deterrent to future cybercrimes.

- **Filing charges:** Based on the evidence collected, charges are framed against the accused under relevant sections of the Information Technology (IT) Act, 2000, and the Indian Penal Code (IPC).
- **Arrest and detention:** Law enforcement authorities may arrest and detain the accused. The duration and conditions of detention are subject to legal procedures and safeguards to protect the accused's rights.
- **Court proceedings:** The case is presented in court, where the prosecution and defense present their arguments and evidence. The court examines the evidence, hears witnesses, and evaluates the legal aspects of the case.

- **Judgment and sentencing:** The court delivers its judgment based on the evidence and arguments presented. If found guilty, the accused is sentenced under relevant IT Act and IPC provisions. Sentences can include fines, imprisonment, or both, depending on the severity of the crime.

Traditional investigation approach



Challenges and roadblocks

- **AI-enabled cybercrime:** The rise of AI has increased the scale and sophistication of cybercrimes, making them harder to detect and counteract.
- **Anti-forensic tools deployed:** Cybercriminals use anti-forensic techniques like disk wiping, file encryption, and steganography to cover their tracks and hinder investigations
- **Unregulated VOIP platforms:** These platforms often lack regulatory oversight, making it easier for cybercriminals to use them for fraudulent activities and evade detection
- **Transnational nature of cybercrime:** Cybercrimes often involve perpetrators and victims in different countries, complicating investigations.
- **Volume of data:** Modern devices can store vast amounts of data, making it time-consuming to sift through and identify relevant evidence.
- **Encryption and anonymity:** Cybercriminals often use encryption and anonymising tools to hide their activities, making them difficult to trace.
- **Legal and jurisdictional issues:** Countries with varying laws and regulations hinder cross-border cooperation and evidence sharing.

Recommendations for enhancing cybercrime investigations in India

01

Outsource forensics services:

Engage forensic experts to handle complex investigations, ensuring their services are integrated within a legal framework for compliance and thoroughness.

03

Concurrent cybercrime investigations:

Allow cybercrime investigations to proceed concurrently, similar to the NIA's involvement in terror cases, ensuring swift and coordinated responses.

02

Dedicated cybercrime police departments:

Establish specialised cybercrime units at both central and state levels, staffed with technically qualified personnel and equipped with modern skills to combat cybercrime effectively.

04

Decriminalise responsible disclosure policy:

Enhance the policy to protect ethical hackers, encouraging them to report vulnerabilities without fear of legal repercussions.

05

Adoption of AI and Machine Learning

While AI has contributed to rising cybercrimes, advanced AI and machine learning tools can enhance threat detection and analysis, strengthening cybersecurity defenses.

06

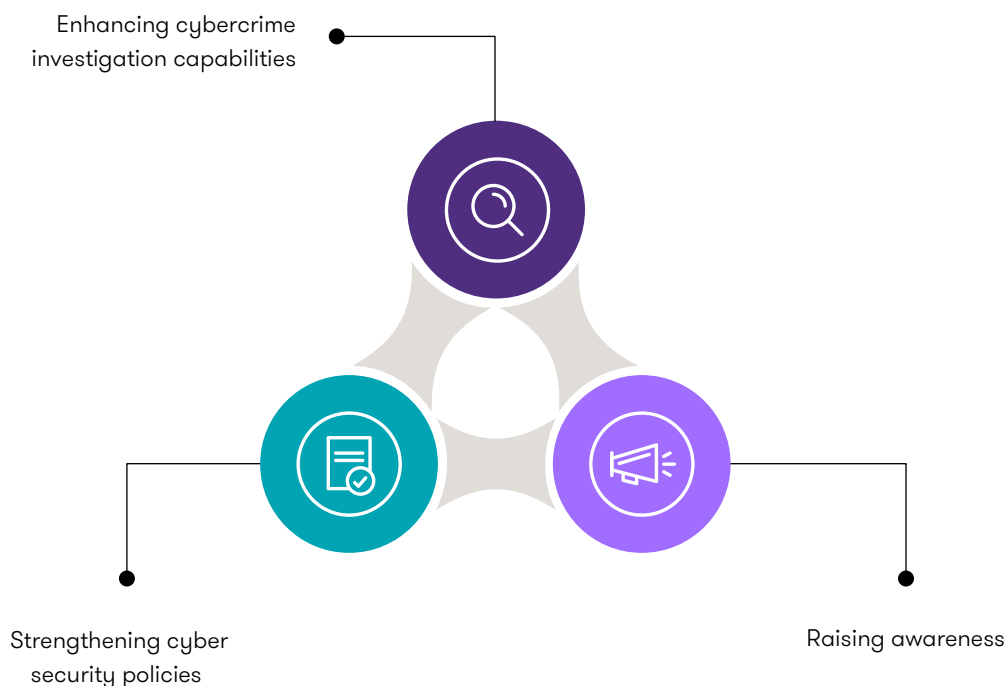
International cooperation and information sharing

Combating transnational cybercrime requires stronger collaboration with global bodies like Interpol and Eurojust, ensuring effective intelligence sharing and coordinated action.



Building upon the proposed framework outlined in the preceding sections, the following recommendations are designed to enhance the effectiveness of cybercrime investigations in India.

These recommendations are divided into three **key areas: Enhancing cybercrime investigation capabilities, strengthening cyber security policies, and raising awareness.**



We can significantly improve the investigative process and outcomes by integrating these actionable steps with the framework's components.

Enhancing investigation capabilities

Strengthening law enforcement's technical capacity

- Provide specialised training programs and recruit dedicated cybercrime experts to enhance the technical capacity of law enforcement agencies. This will equip police forces with the skills and tools to address sophisticated cyber threats.
- Investing in law enforcement agencies' technical capacity will enable them to investigate and combat cybercrimes effectively. This will also help build a robust and capable cybersecurity workforce.

Automated STR generation in banking

- Implement automated Suspected Transaction Reports (STRs) for high-volume transactions in the banking sector to detect and prevent cyber fraud. Immediate action should be taken to freeze suspicious accounts, reducing the risk of large-scale financial fraud.
- Automating the detection of suspicious transactions will enhance financial institutions' ability to identify and respond to potential fraud. This will also help protect customers and maintain the financial system's integrity.

Timely data provision from OTT platforms

- Establish a legal framework to ensure that over-the-top (OTT) platforms like WhatsApp comply with Indian law enforcement requests for data within a specified timeframe. This will help in timely investigations of cybercrimes involving these platforms.
- Ensuring timely access to data from OTT platforms will enable law enforcement agencies to conduct more effective investigations and respond to cyber threats promptly. This will also help maintain public safety and security.

Access to destination IPs from ipv6 networks

- Mandate telecom service providers to store and share destination IP addresses from IPv6 networks with law enforcement agencies. This will facilitate cybercrime investigations by ensuring that online activities can be traced.
- Access to destination IP addresses will enhance the ability of law enforcement agencies to track and investigate cybercriminals. This will also help prevent and address cyber threats more effectively.

Challenges in investigating viral content on WhatsApp

- Compel WhatsApp to provide metadata tagging and source-tracking information for viral content that could lead to societal harm. This will help law enforcement agencies track the spread of misinformation or malicious content.
- Addressing the challenges in investigating viral content will help prevent the spread of harmful information and maintain social harmony. This will also enhance the ability of law enforcement agencies to respond to cyber threats.

Data sharing by local ISPs and cable operators

- Issue a national directive to ensure all Internet Service Providers (ISPs) and cable operators cooperate with law enforcement and share critical data promptly. This will help in tracking cybercrimes more effectively.
- Ensuring cooperation from ISPs and cable operators will enhance law enforcement agencies' ability to gather necessary investigation information. This will also help build a more secure and resilient digital infrastructure.

Inadequate Response from Global OTT Platforms

- Engage global OTT platforms like Twitter, Facebook, and Google to ensure they adhere to Indian law enforcement requirements. Establishing data centres in India could streamline the legal process of data sharing and compliance with Indian jurisdiction.
- Ensuring cooperation from global OTT platforms will enhance law enforcement agencies' ability to conduct effective investigations and help maintain public safety and security in the digital space.

Failure of IMEI Cloning Detection and Prevention Systems

- Require telecom service providers to implement systems that can automatically detect and alert authorities to instances of IMEI cloning. This will help identify and apprehend individuals involved in criminal activities using cloned devices.
- Addressing the issue of IMEI cloning will enhance the ability of law enforcement agencies to track and investigate cybercriminals. This will also help prevent mobile device misuse for illegal activities.



A centralised data-sharing platform for law enforcement

- Create a centralised, real-time data-sharing platform that allows law enforcement agencies to access information from various service providers, ISPs, and platforms. This will enhance investigative efficiency and lead to faster case resolution.
- Establishing a centralised data-sharing platform will improve coordination and collaboration among law enforcement agencies and help build a more effective and efficient system for combating cybercrime.

Banning servers that host malware and illegal content

- Implement stricter regulations to ban servers that host malware or illegal content and penalise virtual private server (VPS) providers that fail to act against illegal activities on their platforms.
- Addressing the issue of servers hosting illegal content will enhance the overall security and trustworthiness of the internet. This will also help prevent the spread of malware and other cyber threats.

Strengthening cyber security policies

Mandatory appointment and role definition of CISOs

- Establish a national framework to ensure the mandatory appointment of Chief Information Security Officers (CISOs) in all organisations. This will provide clear role definitions and enhance cybersecurity leadership, ensuring every organisation has a dedicated person responsible for safeguarding digital assets.
- With CISOs, organisations can better manage and mitigate cybersecurity risks, ensuring a strategic approach to protecting sensitive information. This will also help create a cybersecurity awareness and accountability culture within organisations.

Regulation of third-party vendors

- Develop national guidelines to enforce rigorous security checks for third-party vendors handling sensitive data. This will help prevent data leaks and vulnerabilities introduced by external partners and ensure they comply with industry standards.
- Regular audits and assessments of third-party vendors will ensure that they maintain high-security standards, reducing the risk of data breaches. This will also foster a sense of responsibility among vendors to prioritise cybersecurity in their operations.

Digitisation of asset registers and risk management

- Initiate a nationwide effort to digitise asset registers and implement robust risk management practices in government departments. Maintaining real-time records of digital assets will help proactively identify and mitigate cyber threats.
- Digitising asset registers will enable better tracking and management of government assets, ensuring that vulnerabilities are identified and addressed promptly. This will also facilitate more efficient resource allocation and risk management.

Strict KYC regulations

- Enforce strict Know Your Customer (KYC) regulations across all financial institutions, including physical verification of documents. Establish a centralised database for KYC verification to prevent fraud and money laundering by ensuring all accounts are verified and traceable.
- Strengthening KYC regulations will help curb financial crimes and ensure that only legitimate individuals and entities can access financial services. This will also enhance the overall security and integrity of the financial system.

Creation and implementation of Cyber Crisis Management Plans (CCMP)

- Mandate developing and implementing Standard Operating Procedures (SOPs) and Cyber Crisis Management Plans (CCMP) for all states and sectors. This will ensure a coordinated and swift response to any cybersecurity breach, minimising damage and recovery time.
- Having well-defined SOPs and CCMPs will enable organisations to respond effectively to cyber incidents, reducing the impact on operations and services. This will also help in building resilience and preparedness for future cyber threats.

Regulation of VPN Services

- Introduce a regulatory framework to control VPN usage, including mechanisms to detect and track multi-chained VPN networks used for illegal activities. This will help law enforcement agencies trace cybercriminals who use VPNs to hide their identities.
- Regulating VPN services will ensure that they are not misused for illegal activities while still providing privacy and security for legitimate users. This will also help balance privacy and security in the digital space.

Regulation of Public and Shared Wi-Fi Networks

- Implement a system to mandate the collection of basic user metadata, such as MAC addresses, when utilising public Wi-Fi networks. This will aid in investigations of serious offences by ensuring that users of public networks can be identified if necessary.
- Ensuring the security of public and shared Wi-Fi networks will protect users from cyber threats and enhance the overall safety of the digital environment. This will also help prevent cybercriminals from exploiting these networks for illegal activities.

Improvement of Location-Based Services (LBS)

- Upgrade LBS accuracy, especially in remote areas, to aid law enforcement agencies in tracking suspects or victims more effectively. This will involve working with service providers to ensure that location data is precise and reliable.
- Enhancing LBS accuracy will improve the effectiveness of law enforcement agencies in conducting investigations and responding to emergencies. This will also help provide better services and support to citizens in remote and underserved areas.



Cooperation from domain registrars

- Engage with international domain registrars to ensure cooperation with Indian law enforcement agencies. Empower state governments to block malicious domains promptly, expediting the removal of harmful websites from the internet.
- Ensuring cooperation from domain registrars will help quickly address cyber threats and prevent the spread of malicious content. This will also enhance the overall security and trustworthiness of the Internet.

Regulation of cryptocurrency exchanges

- The Reserve Bank of India (RBI) should regulate all cryptocurrency exchanges and mandate annual audits to ensure compliance with anti-money laundering (AML) and financial transparency requirements. This will help curb the use of cryptocurrencies for illegal activities.
- Regulating cryptocurrency exchanges will ensure that they operate within the legal framework and adhere to high security and transparency standards. This will also help in preventing the misuse of cryptocurrencies for money laundering and other financial crimes

Raising cyber awareness among citizens

Enhanced cyber hygiene training for government employees

- Implement comprehensive training programs to improve cyber hygiene practices among government employees. This will focus on protecting systems from malware, phishing, and ransomware attacks, ensuring that government infrastructure remains secure.
- Enhancing cyber hygiene among government employees will reduce the risk of cyber incidents and improve the overall security of government systems. Regular training sessions and workshops will keep employees updated on the latest cybersecurity threats and best practices, fostering a culture of vigilance and responsibility.

Public awareness campaigns

- Launch nationwide public awareness campaigns to educate users on recognising genuine government websites and avoiding scams. This will help reduce fraud, particularly in passport services and driving license applications.
- These campaigns should utilise various media platforms, including social media, television, and print, to reach a wide audience. By providing clear and practical information, such as identifying phishing emails and securing personal information online, these campaigns can empower citizens to protect themselves against cyber threats.

Automated action against bulk SMS fraud

- Develop automated filters to detect and block fraudulent bulk SMS messages containing keywords like "jackpot," "lottery," or "work from home." This will protect users from phishing attacks and other scams through bulk SMS campaigns.
- Implementing these filters will significantly reduce the number of fraudulent messages reaching users, decreasing the likelihood of individuals falling victim to scams. Additionally, educating the public about the dangers of responding to such messages and encouraging them to report suspicious SMS can further enhance protection.

Regulation of disposable email addresses

- Regulate the use of disposable or temporary email addresses to prevent cybercriminals from creating fake accounts on various online platforms. Ensuring all user accounts are traceable will help reduce online fraud and other illegal activities.
- By requiring online platforms to verify email addresses and restricting the use of disposable emails, the government can make it more difficult for cybercriminals to operate anonymously. Public awareness initiatives can also inform users about the risks associated with disposable email addresses and encourage them to use secure, verified email services.

Awareness of fake websites:

- Increase efforts to educate the public on differentiating between legitimate and fake websites. This will involve issuing guidelines and conducting awareness campaigns to help users avoid scams.
- Providing tools and resources, such as browser extensions and online verification services, can assist users in identifying fake websites. Regular updates and alerts about new types of scams and fraudulent websites can keep the public informed and vigilant, reducing the risk of cyber fraud

Conclusion

In conclusion, the cybercrime landscape in India faces numerous challenges that require immediate and coordinated action. The proposed measures—strengthening cybercrime policies and investigation capabilities and raising cybercrime awareness among citizens—provide a comprehensive approach to addressing these issues. By implementing these measures, India can significantly improve its ability to combat cybercrime and protect its citizens from evolving threats.

- Strengthening cybercrime policies and investigation capabilities – Establishing specialised cybercrime units, enforcing stricter KYC regulations, regulating VPN services, and equipping law enforcement with better training and tools will enhance India's ability to combat cyber threats effectively. A centralised data-sharing platform will further improve coordination among agencies, leading to faster case resolutions.
- Raising cybercrime awareness among citizens – Public education campaigns, cyber hygiene training, and awareness about online risks such as cyberstalking, scams, and sextortion will empower individuals to protect themselves and contribute to a safer digital environment. Regulating disposable email addresses and improving cyber hygiene training for government employees will further strengthen cybersecurity efforts.

By addressing these critical areas, India can create a safer and more secure digital ecosystem. The collective efforts of government bodies, law enforcement agencies, private organisations, and citizens are essential for achieving this goal. Through collaboration and proactive measures, India can strengthen its cybercrime response and safeguard its digital infrastructure for the future.

References:

Press Information Bureau
National Crime Records Bureau
Cyber Digest by Indian Cyber Crime Coordination Centre
World Economic Forum
Indian Cyber Crime Coordination Centre
Ministry of Electronics and Information Technology (MeitY)
Data Security Council of India
Federal Trade Commission
Cloudflare, Inc.

Glossary of key terms

FCRF	Future Crime Research Foundation
NCRB	National Crime Records Bureau
NCRP	National cybercrime reporting portal
OSINT	Open-source intelligence
OTP	One time password
KYC	Know your customer
FIR	First information report
MHA	Ministry of Home Affairs
I4C	Indian Cybercrime Coordination Centre
AI	Artificial intelligence
AIIMS	All India institute of medical sciences
UPSRTC	Uttar Pradesh State Road Transport Corporation
BBPS	Bharat bill payment system
CIS	Cyber and Internet security
NCB	Narcotics control bureau
CCTNS	Crime and criminal tracking network and systems
CCTNS-JMIS	Crime and criminal tracking network and systems – Jurisdiction management information system
JCCT	Joint Cybercrime Coordination team
CERT	Computer emergency response team
NCIIPC	National Critical Information Infrastructure Protection Centre
DIR	Digital forensics and incident response

Acknowledgements

For more information contact:



Prof. Triveni Singh

Ex IPS, Chief Mentor FCRF
E: triveni@futurecrime.org



Ramendra Verma

Partner and Leader, Government sector
E: ramendra.verma@in.gt.com



Akshay Garkel

Partner and Leader, Cyber
E: akshay.garkel@in.gt.com



Gaganpreet Singh Puri

Partner and Leader, Forensic
E: gagan.puri@in.gt.com

Contributors:

Jitendra Singh

ACP

Ankush Mishra

DySP Uttarakhand Police

Mithilesh Jha

Sub Inspector , UP STF

Shashank Shekhar

Co-Founder, FCRF

Harshvardhan Singh

Co-Founder, FCRF

Titiksha Srivastav

Associate, FCRF

Swagta Nath

Associate, FCRF

Achintya Seshadrinathan

Manager, Grant Thornton Bharat

Sagar Gajara

Manager, Grant Thornton Bharat

Editorial Review

Shabana Hussain

Design

Jatin Arora



We are Shaping Vibrant Bharat

A member of Grant Thornton International Ltd, Grant Thornton Bharat is at the forefront of helping reshape the values in the profession. We are helping shape various industry ecosystems through our work across Assurance, Tax, Risk, Transactions, Technology and Consulting, and are going beyond to shape more **#VibrantBharat**.

Our offices in India

- Ahmedabad ● Bengaluru ● Chandigarh ● Chennai
- Dehradun ● Goa ● Gurugram ● Hyderabad ● Indore
- Kochi ● Kolkata ● Mumbai ● New Delhi ● Noida ● Pune



Scan QR code to see
our office addresses

www.grantthornton.in

Connect
with us on



@Grant-Thornton-Bharat-LLP



@GrantThorntonBharat



@Grantthornton_bharat



@GrantThorntonIN



@GrantThorntonBharatLLP



GTBharat@in.gt.com

© 2025 Grant Thornton Bharat LLP. All rights reserved.

Grant Thornton Bharat LLP is registered under the Indian Limited Liability Partnership Act (ID No. AAA-7677) with its registered office at L-41 Connaught Circus, New Delhi, 110001, India, and is a member firm of Grant Thornton International Ltd (GTIL), UK.

The member firms of GTIL are not a worldwide partnership. GTIL and each member firm is a separate legal entity. Services are delivered independently by the member firms.

GTIL is a non-practicing entity and does not provide services to clients. GTIL and its member firms are not agents of, and do not obligate, one another and are not liable for one another's acts or omissions.