Development in Electronic Media has Given Rise to Computer Related White Collar Crime

S. Anbuselvi

Paper Number: 240074

Abstract:

Electronic media has forthrightly ticketed the nature and scope of white-collar crime, creating new problems for victims, regulators, and law enforcement in India and worldwide. The digitization of communication, monetary transactions, and personal information has enabled criminals to engage in extensive economic crimes - including identity theft, cyberspace fraud, blackmail, and corporate manipulation - often without detection or direct interaction with victims. The omnipresence of the internet, the proliferation of digital banking and social media, has made cybercrimes, phishing, data breaches, online scams, and electronic marketplace manipulation easier to engage in and easier to escape from, often perpetrated by an individual working within government agencies or corporations, exploiting legal loopholes and technological advancements. The consequences can be severe for victims, they can suffer financial loss, reputational impact, and mental anguish. For companies they can incur additional costs, suffer damage to their reputation and experience loss of public trust/downgrading by regulators. Governments cannot keep track of rapidly evolving cyber techniques. Certain legislation such as the Information Technology Act, 2000 and the Prevention of Money-Laundering Act, 2002 has attempted to address these offences; however, enforcement is often impeded by lack of awareness, slow pace of justice and difficulty obtaining digital evidence. The example of prominent Indian cases of the Paytm, blackmail case and the fake website for Amazon show the scope and complexity of these offenses. As electronic media change and evolve, so too must laws, policies, and public awareness campaigns to address the increasing threat of white-collar crime rise in the digital age.

Keywords*: white-collar crime, electronic media, cybercrime, identity theft, digital fraud, regulatory challenges, Indian legislation, Information Technology Act, economic offenses, corporate manipulation.*

Introduction

"It's not enough to protect your data; you need to protect your customers' data too."

– Satya Nadella[1]

Cyber-crimes have initiated a fresh discussion regarding the need for new laws to address white-collar cyber-crime or if the current legal framework is adaptable enough to manage this emerging form of criminal activity committed by individuals with high intelligence. A group of thinkers holds that cyber-crimes are not fundamentally different from traditional offenses such as trespass or conspiracy, except that in some instances, a computer has served as a tool or medium for committing the crime.[2] The other School places great emphasison the distinctive characteristics of emerging technologiesand the specific challenges, unfamiliarto current criminal law, s uch as the nature and extent of cybercrimes, the internet, and identifying an offender's location, jurisdiction, and enforcement issues. It argues that a new allen compassing law is required to address cyber-crimes.[3]Typically, nations that are keen on combating cyber-crime have employed two distinct strategies to address it: viewing cyber-crime as conventional offenses involving advanced technology and recognizing it as a unique type of crime that necessitates a new legal framework.[4] The remarkable expansion of the Internet has created a new landscape for cybercrimes. The increase of cyber-crime cases (under the Information Technology Act and the Indian Penal Code) by 69.0% compared to 2013 (i.e., 5,693 in 2013 to 9,622 in 2014)[5]. The National Crime Records Bureau (NCRB) most recently reported that, in 2014, 9,622 cyber-crime occurrences rose in 2014 to last year (i.e., 2015) 11,592 cases and that about one-third of these offences were financially motivated.[6]

A new wave of crime has emerged with the arrival of the Internet. Computer hacking, software theft, online child exploitation, corporate spying, password cracking, spoofing, telecommunications scams, email flooding, spamming, adult content and the presence of illegal or unregistered goods and services constitutes offenses that haveal ready left their impact.[7] New

[1]CEO of Microsoft

[2]Watkins is of the opinion that the hard evidence of the extent of such crimes and the need for specific legislation directed at computer crime is still lacking. See Watkins, Computer crime: Seperating the Myth from reality, C.A. Magazine, January1981.

[3] Parker believes that the challenges posed by the computer crime have made the existing legal regime inapplicable and ineffective. See Parker, Computer Abuse Research Update, 2 Computer L.J. 329-523(1980).

[4] In America 31 States have passed new legislations to deal with computer related crimes whereas others have amended the definition of Larency to include electronic media. See Michael D. Rostorker et al. Computer jurisprudence, Legal Response to the Information Revolution (1986)

[5]Cyber Crime Bureau Compendium 2014

[6] Times of India on 31st August 2016.

[7] B.B. Nanda R.K. Tiwari,‖ Cyber crime-A Challenge to Forensic Science, the Indian Journal, April-Sept. 2000 at 103.

challenges arising include credit carddeception, online terrorism, and digital money laundering and unlawful exploitation of secure internet communications.[8] The current fragile electronic payment system lacks sufficient the safeguard presents a significant threat of unauthorized withdrawals from banks and counters.

Software piracy is a thriving enterprise, and the video and phonographic sectors are declining daily on a global scale.[9] It is now clear that substantial sums of money are illicitly transferred from one location to another by tech-savvy criminals, either through damaging computer systems, stealing valuable information, or engaging in other unlawful activities enabled by networks. The inquiry is what constitutes a computer crime? Neither the Indian Penal Code nor the IT Act provides a definition for it. The latest changes to the Indian Penal Code render specific actions punishable without explicitly labelling them as computer crimes.[10]

Defining computer crime has faced numerous challenges in different jurisdictions because, there has been a great deal of disagreement about the scope and limits of the definition.[11] Also, the term "computer crime" or "computer misuse" lacks an exact definition, and generally consists of a broad range of crimes related to computers,[12] which may include, for example, unauthorized access of computers and stored data, damage to computer-stored information, trafficking in passwords and hacking tools, making and distributing unauthorized copies of software, and sending spams or pornographic images.[13]

Evolution of Computer Related White Collar Crime

White collar crime is a fairly recent development in the field of criminal science. Even though Certain crimes, such as bribery and other forms of corruption, were prevalent in India during both the Hindu and Muslim eras, and Western nations like the United States, European countries, and Britain have experienced them since their inception.[14] Nevertheless, the current investigation of white-collar crime results from research carried out by the late Professor Edwin Sutherland. He released his first significant study of white-collar offenses perpetrated by seventy of the two hundred largest non-

[8] Ibid.

[9] David Teather Pirates Sink Music Firms, HT April 21,2001

[10]Michael Rostoker opined that the underlying difficulties present in legislating and enforcing effective criminal statutes is the uncertainty as to the definition and scope of what constitutes a computer crime. Supra note .1See also Marc D Goodman, Why the police do not care about computer crime. Harv. J of computer Technology, vol.10,No.3(1997),466.

[11]Taber on computer crime(Senate Bill 5240)1 Computer L.J.517(1979).Also see, PA, Collier and BJS Paul, Problems in policing computer crime ,2,Policing and Soc'y (1992).

[12]General Accounting Officer, Computer related crime in Federal Programmes 1 (1976).

[13]Indira Carr, India join the cyber-race: Information Technology Act, 2000.

[14] Government of India, "Report of the Commission on the prevention of corruption" (1964)para2.3.Kautilya in his Arthasastra refers to various kinds of corruptions prevalent during that time ;See Law Commission of India, "29th Report: proposal to in clued Social and Economic offences in the Indian penal code", Pp. 1-9.

official corporations in the United States between 1940 and 1950. The research uncovered thescale of different types of anti-social behaviour common in America thatwas being carried out by individuals of elevated social standing and reputation while pursuing their careers.[15]

The notion of white-collar crime is based on a socialist, anti-business attitude that characterizes it and cites the socioeconomic class of people of who it vilifies. While Edwin Sutherland is noted as having first studied white-collar crime, the discipline of white-collar crime and the idea of white-collar crime did not develop independently of one another. The importance of understanding different manifestations of white-collar wrongdoing has a deeper purpose through explaining the creation of the idea of white-collar crime and describing its developments. White-collar crime has been defined in numerous ways, including asa wrongdoing committed by anindividual of esteemed or elevated social status, or as anoffense committed during one's profession, along with an illegal act related todeceit or a breach of trust, classified as a non-violent crime committed for personal gainprofit, as an offense that encompasses a mix of these elements and merely as enter priseoffense.[16]

Another significant occurrence that has intensified the issue of these criminal activities lately is the notion of economic globalization. Globalization is the increasing truth of contemporary times. The idea of globalization has altered the social, economic, and political dynamics between the Nations around the globe and the world have turned into a global community. The occurrence the rise of globalization has led to an increase in trade, greater mobility, and the opening up of economy, elimination of control mechanisms and thinking in liberalization. Innovation progress and creativity have significantly increased recently, and we have been impacted by such alterations. As a result, dealing in drugs and narcotics, weapons and bomb trade, fake financial contracts, currency exchange Manipulations and additional offenses are creating new dimensions within the criminal landscape. Consequently, emerging unlawful actions like money laundering and 'trading in "Crime proceeds" have surfaced, creating illicit funds or underground economies and risking the country's fiscal stability.[17]

The history of white-collar crime in India shows a gradual transition from traditional corporate fraudulent crimes to fraud crimes enabled through the usage of technology in the 21st century, where technology serves as an enabler and a weapon to criminals. More than 4,599 fraud cases were registered in India with the amount of Rs.1203 crore in early 2024, further complicating the criminal justice process surrounding the commitment,

[15] K.D. Gaur Criminal law and criminology 280 (Deep and Deep Publication pvt.Ltd.,1ST edn.,2002)
[16] Sanjeev Mahajan, Criminology and penology 68 (Arjun Publishing House, New Delhi, 1 stedn.,2008)
[17] National Crime record Bureau, (MHA) "Crime in India (1994) Economic Offences" P. 327.

prevention, and prosecution of such crimes. Either through oral or written recording, antiquity from the Indian texts, and the colonial records, show examples of multiple acts of corruption including bribery, forgery, and other alterations to the financial structure—now occurring on digital platforms with global connectivity.

Types of cyber crime

1. Identity theft
2. Social engineering
3. Botnets
4. Phishing
5. Cyber stalking
6. Digital arrest

Role of Electronic Media in Facilitating White-Collar crime

Digital fraud and identity theft: Criminals use electronic platforms for phishing, social engineering, and malware/ransomware attacks to steal sensitive information, extort funds, and corrupt corporate data. For example, common "phishing" scams use emails or fake websites to trick people into revealing financial information.

Anonymity and remote Offending: Perpetrators have the ability to commit offenses from afar without physical proximity. Criminals often exploit the anonymity and diminished chance of detection. For example, instant messaging, encrypted sites, and social media are frequently used to mask transactions and fraudulent communications.

Money Laundering with Crypto-Currency: Electronic currencies and online trading platforms provide rapid and cross-border processing that does not give authorities time to identify and shut down payment processing and financial crime committing banks, giving criminals a chance to complete their laundering of illicit proceeds.

Rapid Transaction: Modern digital currency banking and crypto-currency allows for almost instantaneous cross border transmission of funds as digital currency provides minimal traceability for law enforcement recovery of the proceeds of crime.

Examples

Salami Attacks: Small unauthorized deductions from account balances or discreetly applied to transactions build up quickly over time. Knowledge of these deductions was demonstrated in the Ziegler case and more recently in ransomware incidents like WannaCry.

Corporate Data Manipulation: Corporate members or outsiders manipulate corporate databases and records of transactions remotely causing millions

in corporate fraud, as was evidenced in the IL&FS crisis and the (Punjab National Bank) PNB scam.

Online Market Manipulation and insider trading: Social media and online forums are used in various ways to distribute false information, coordinate illegal trades, do market manipulation, etc.

Judicial Prouncement

Development in electronic media has directly accelerated the growth ofcomputer-related white-collar crimein India, leading courts to address evolving issues in cyber fraud, data theft, intermediary liability, and electronic banking fraud through several landmark case laws in recent years

SBI Electronic Banking Fraud Case[18]

The Supreme Court upheld the Gauhati High Court's order directing SBI to compensate a customer for losses suffered due to unauthorized electronic banking transactions, affirming that banks hold liability if fraud is reported promptly by customers. The Court relied on RBI's July 2017 circular, clarifying customer protection in electronic transactions.

This landmark Supreme Court decision struck down Section 66A of the IT Act, finding it vague and unconstitutional. It protected freedom of speech online by limiting criminalization of "offensive messages" sent through electronic media.[19]

Bazee.com case[20]:The CEO of Bazee.com was held liable for hosting obscene content online, leading courts to clarify intermediary liability under Section 79 of the IT Act. This judgment shaped safe harbour protections for tech platforms.

Sony Sambandh Case[21]: This was India's first conviction for cyber fraud involving online purchase through stolen credit card information. The accused was found guilty under Sections 418, 419, and 420 IPC for using electronic media to perpetrate white-collar crime.

The Supreme Court clarified intermediary liability for defamatory content published by third parties on digital platforms, emphasizing platform responsibility in moderating electronic media content.[22]

Impact and Contemporary Relevance

Recent judgments show courts holding financial institutions and tech companies accountable for digital fraud, data breaches, and content moderation, recognizing the evolving risks posed by electronic media.The Supreme Court's affirmation of privacy and the RBI guidelines protect users from unauthorized data use and enforce stronger compliance among

[18]Special Leave to Appeal (C) No. 30677/2024, Supreme Court of India, Judgment dated 3rd January 2025
[19]Shreya Singhal v. Union of India
[20]Avnish Bajaj v. State (2008) 150 DLT 769 (Del)
[21]CBI v. Arif Azim (Sony Sambandh Case) (2013)
[22]Google India Pvt. Ltd. v. Visaka Industries (2020)

electronic media operators.Convictions under IPC and the IT Act demonstrate Indian law's adaptability to new forms of white-collar crime driven by electronic media.

Identity Theft case:

The Amar Singh and Neha Punjani-Singh case is known as one of the largest identity theft and credit card scams in U.S. history, involving a sophisticated criminal network that operated across multiple states and countries.

Amar Singh and his wife, Neha Punjani-Singh, masterminded a $13 million fraud scheme centered on identity theft and enterprise corruption. The operation led to the arrest of 111 individuals and spanned from July 2010 to September 2011. The criminals used skimming devices to steal credit card information from unsuspecting victims when making purchases at restaurants or retail outlets. The stolen data was used to create counterfeit cards that enabled "shoppers" to spend lavishly on luxury goods, hotel stays, car rentals, and even private jets. Personal data sources included foreign suppliers from countries such as Russia and China as well as U.S. based accomplices.

Legal Proceedings and Sentencing

- Both Amar Singh and Neha Punjani-Singh pleaded guilty to charges of identity theft and enterprise corruption.
- Amar Singh, cited as one of the four ringleaders, faced a possible sentence of up to 250 years but was ultimately sentenced to 5⅓ to 10⅔ years in prison.
- Neha Punjani-Singh pleaded guilty to petty larceny and received a conditional discharge sentence, avoiding severe punishment due to Singh's plea agreement.

Impact and Legal Commentary

- This case highlighted gaps in the criminal justice system concerning cybercrime prosecution, as sentences were viewed as lenient given the massive financial losses and the number of victims involved.
- The FTC estimated the cost of identity theft to Americans was around $1.52 billion in 2011, underscoring the significance of these crimes.
- The judge publicly reprimanded Singh for his exceptional deceit, calling him a "huge criminal" and "rip-off artist extraordinary".
- The case contributed to public awareness regarding the use of credit card skimming devices and the importance of monitoring personal financial data.

- Experts recommend credit freezes, careful reviewing of monthly statements, and vigilance when using cards at ATMs or point-of-sale machines to reduce risk.

Amar Singh and Neha Punjani-Singh orchestrated a massive, international identity theft ring ultimately convicted and sentenced in New York for their roles in a $13 million scam involving credit card fraud, luxury spending sprees, and hundreds of victims. Despite facing severe charges, both received relatively lenient sentences within the context of U.S. cybercrime law enforcement.

The case of **MGM Resorts** identity theft pertains to two high visibility data breaches in 2019 and 2023, which exposed sensitive information from millions of guests and resulted in various class action lawsuits and a $45 million settlement.

In July 2019, hackers accessed the computer systems of MGM Resorts International without authorization and extracted guest personally identifiable information (PII) such as the names, addresses, phone numbers, emails, dates of birth, driver's license numbers, passport details, and military identification (ID) numbers of its guests.

The stolen data was advertised for sale on darknet forums; in addition, criminals used the stolen data to commit identity theft, falsely file tax returns, register for accounts, and phishing for valuable additional information.

Initially, it was estimated that 10.6 million guests were affected, but additional reports caused the estimation to rise to 142 million individuals.

In September 2023, MGM faced a ransomware attack that resulted in affecting over 37 million customers and shutting operations down for several days for its properties in Las Vegas, including the Bellagio and Aria hotels.

The attackers employed social engineering methods, impersonated a company employee to access the network, and continued to gain customer information by exploiting additional vulnerabilities, which included Social Security numbers, passport numbers, and driver's license numbers.

Legal Suit and Settlement

Plaintiffs contended that MGM did not implement appropriate cybersecurity measures, opening up the organization's highly sensitive and valuable data to the public.

Lawsuits resulting from these data breaches were merged into multi-district class action cases in the United States District Court for the District of Nevada, affecting millions of individuals who claimed to be impacted.

In early 2025, MGM reached a $45 million settlement for a class action, which a judge approved on June 18, 2025.

Settlement funds will be dispersed based on their damages (a reimbursement for documented damages), as well as cash payments based

on the extent of their exposure ($75 for social security/military ID exposure, $50 for passport/driver's license exposure, and $20 for basic information leaks) to participating victims, along with free credit monitoring offered to impacted guests.

The case highlights the ongoing systemic vulnerability of the hospitality industry and the need for stronger data security practices.

It established new norms for businesses' obligations related to cybersecurity and financial relief for the victims of identity theft through the civil justice system.

The breach and subsequent class action settlement reinforces that attackers take advantage of both technical flaws and human error in an industry that exposes consumers to risk in a very significant way.

Social Engineering

A social engineering attack in cybersecurity involves using psychological manipulation to trick individuals into revealing sensitive information, downloading malware, or performing actions that compromise their security.

Common Types of Social Engineering Attacks

Phishing: The use of scam emails, messages, or websites that appear to come from a trusted source to capture credentials or personal information.

Pretexting: The use of a fabricated story or scenario to deceive the target and build trust to gain information.

Baiting: The ability to place a lure, although it may be enticing, to trick a client to lower their guard and give up security.

Tailgating/Piggybacking: The act of sneaking into a restricted area by following and authorized person.

Whaling: A type of phishing that specifically targets high-profile executives within a corporation.

Vishing: Voice phishing; criminal actors utilize phone calls and pose as legitimate organizations in order to collect sensitive information.

Smishing: SMS phishing; informing victims of text messages to input personal information and/or access malicious sites.

National Association of Software and Service Companies vs. Ajay Sood & Others (Delhi High Court, 2005)[23]

Facts: The defendants used the name "NASSCOM" in e-mails (fraudulent e-mails) to extract personal data, under the guise of a head-hunting / recruitment agency. This is a sort of phishing / impersonation scam. Though there was (at that time) no specific statute defining "phishing," the court treated it as illegal under principles of **passing off, misrepresentation**, trade mark infringement, etc. The court granted

[23]119 (2005) DLT 596.

permanent injunction, damages, etc. First major Indian case to define phishing legally, also to attach legal liability for social engineering via emails.

Conclusion

The rise of electronic media has changed white-collar crime, creating new types of computer-related offenses that are more complicated, widespread, and harder to detect. These crimes, like cyber fraud, hacking, identity theft, and data breaches, take advantage of the anonymity, speed, and global reach that digital technologies provide. This evolution has put pressure on traditional legal and investigative methods, leading to a need for urgent updates to address the new threats effectively. The economic and social effects of these crimes are serious; they disrupt financial systems, erode trust, and result in significant losses for individuals and organizations.

To tackle these challenges, we need to update legal policies to include specific cybercrime laws and improve forensic and technical skills among law enforcement agencies. Using technologies like artificial intelligence, blockchain, and encryption can help enhance detection and prevention efforts. It's also important to promote cooperation between government, the private sector, and universities to share knowledge, train staff, and develop solid cybersecurity plans. At the same time, educating the public about cyber threats and best practices through ongoing programs is crucial to minimizing vulnerability.

In summary, addressing computer-related white-collar crime needs a broad strategy that includes legal reforms, technological advancements, collaboration among institutions, and public involvement. This approach is essential for creating a strong digital environment that can protect against new cyber threats in today's electronic media age. Such a response is vital for maintaining social order and economic stability in our increasingly digital world.

Suggestions

- Regularly upgrade and adapt digital forensic tools to match the evolving tactics of cyber offenders, while emphasizing integration with current investigative technologies.
- Foster structured collaboration among law enforcement, private sector, and academic institutions to share expertise, conduct joint training, and enhance digital forensic methodologies.
- Mandate cybersecurity awareness campaigns and employee training programs as integral to organizational practice, encouraging the development of a culture of vigilance and adoption of best security protocols.

Advanced Technology Solutions

- Deploy artificial intelligence (AI) and machine learning to detect fraudulent patterns, network anomalies, and suspicious transaction behaviors.
- Implement automated identity verification tools, facial analysis, and document scanner solutions to reduce identity fraud and secure digital interactions.
- Utilize blockchain technology for transparent, tamper-proof record-keeping in sensitive financial and data transactions

Institutional Measures

- Conduct thorough background checks on employees, contractors, and third-party service providers before granting access to critical systems or confidential data.
- Perform regular internal and external audits, supplemented by continuous monitoring of financial and operational activities to flag inconsistencies and abnormal behaviors.
- Develop clear internal policies and standard operating procedures to respond swiftly to suspected cybercrime incidents.

Organizational and Public Awareness

- Institute mandatory, ongoing cybersecurity training for employees to minimize human error and raise awareness of phishing, social engineering, and other common attack vectors.
- Run public awareness campaigns through media and civil society initiatives about online fraud risks, protective measures, and reporting procedures.