LAWFOYER INTERNATIONAL JOURNAL OF DOCTRINAL LEGAL RESEARCH

(ISSN: 2583-7753)

Volume 2 | Issue 2

2024

FROM CLICK TO CONSEQUENCES: INVESTIGATING THE CYBER CRIMES' TRAIL IN BUSINESS

Sushree Sangita Panda[1]

I. ABSTRACT

The developing nature of technology and digital generation has converted business operations into smooth and reliable one, but it has also exposed them into an increasing threat landscape. The generalization of cybercrime in today's digital eco system creates substantial concerns to the organizations across the globe. This research paper digs into the complex web of cybercrime and its extensive consequences for numerous aspects of corporate operations. This paper explores the ever-evolving nature of cyber risk, which revolves from the basic clicks to the subsequent commercial ramification, thru an investigating prospective. This study illuminates the various consequences of cyber-crime by examining the actual-world instances and business movements. This also highlights the multifaceted effects of cyber-crime in business which includes financial losses, operational interruption, data breaches, IP thefts, reputation harm etc. On top of that this paper also investigates solutions for reducing cyber risks and increasing resilience in the context of persistent attacks. Last but not least, this research intends to develop understandings of the critical interplay of cyber-crimes and businesses as well by providing insights to protect the digital vulnerability and fortify the organizational defence.

II. KEYWORDS:

Cyber security, corporate, digital eco-system, data thefts, technology.

III. INTRODUCTION

Businesses all around the planet are becoming more dependent on technological advances and networks in order to generate innovative thinking, efficiency, and

[1] Birla Global University, Bhubaneswar

 (ISSN: 2583-7753)

competitiveness in the age of the internet. On the other hand, these developments have been accompanied by the rising menace of cybercrime, that presents substantial hazards to organisational protection and profitability. Cybercriminals, equipped with proficient equipment and tactics, use weaknesses in technology to conduct assaults that can have serious ramifications for enterprises. Businesses are becoming more dependent on technological advances to simplify procedures, extend their reach in the marketplace, and boost efficiency in an age of digital connectedness.

In contrast, growing reliance on technology exposing organisations to a wide range of cyber dangers, from advanced hacking techniques to harmful software assaults. Cybercrime has evolved as a powerful threat to organisations of all sizes and industries, providing major operational, monetary, and reputational hazards. No organisation, from tiny businesses to giant enterprises, is exempt to cybercriminals' ubiquitous grasp. The expression "from clicks to consequences" captures the core of the cybercrime path that firms must navigate. It starts with a seemingly unimportant just to click—a URL in a mail message, downloading from an unidentified source, or an excursion to a hacked website.

However, the ramifications of acts like this can resonate within an organisation, resulting in an infinite chain of negative outcomes. The effect of cyber-crime is continuously visible in every part of the company Either it's monetary losses from forged transactions, administrative interruptions from incidents involving ransomware, or adverse reputational effects from breaches of information. It is critical to enable organisations to proactively manage cyber risks and protect assets while assuring consistency, reliability, and profitability in a rapidly computerised environment.

IV. RESEARCH OBJECTIVES

1. To Determine the monetary effect of cybercrime on enterprises, encompassing immediate cash damages, functional interruptions, and future financial effects.

2. To investigate the problem of stealing intellectual property in light of cybercrime, particularly theft of business techniques and research information, as well as its effect on creativity and competitiveness.
3. To investigate the reputational harm done to enterprises as a consequence of cybercrime, including the destruction of client confidence, reputation for brands, and measures for managing their reputations and rehabilitation.

V. RESEARCH QUESTIONS

1. What are the ramifications of cyberattacks for the organisation security and confidentiality of data, and what is the impact of that on compliance with regulations and confidential details safeguarding?
2. How can organisations deal with the complex problem of brand harm, adherence to regulations and laws, and possible repercussions caused by a cybercrime?
3. How can organizations assess their safety in assets and strategy as they respond to new cyber hazards? What practical guidance can help enhance cyber resilience and reduce potential hazards of cybercrime?

VI. RESEARCH HYPOTHESES

1. Cyberattacks are a serious danger to organisational well-being in the present economic climate. Data theft, which is a typical type of cybercrime, destroys confidential data and discloses highly confidential financial or personal data. This can result in consequences from authorities enforcing stringent data security requirements, diminished public trust, probable income loss, and a tarnished brand. System complications caused by cyberattacks can potentially impair critical business processes. Cybercrime's economic impact includes costs for recovering information, forensic assessments, branding restoration, and potential lawsuits. To reduce these risks, businesses must employ creative cybersecurity policies that ensure regulatory compliance and build resilience in the continually evolving cybercrime risk landscape.
2. The organization needs to investigate solutions to reduce the damaging effects of cybercrime, with an emphasis on corporate image governance, compliance with

laws and regulations, and legal concerns. A timely reaction is critical for brand rehabilitation, and organisations should include stakeholders to create a comprehensive depiction of the event and restoration actions. Public relations experience may help you offset adverse coverage and launch strategic messages to reestablish trust. Adherence with data protection rules such as GDPR or CCPA necessitates an extensive conformity evaluation that identifies communication needs and constraints. Consulting with cybersecurity specialists can assist in identifying possible risks and determining effective solutions. Cybersecurity insurance can provide financial protection from legal liabilities. Organisations can manage cybercrime, minimise long-term harm, and emerge more resilient by taking a comprehensive strategy and prioritising proactive cybersecurity measures.

3. Organisations managing the ever-shifting tides of cyber assaults require a comprehensive approach for assessing asset in security and strategic readiness. Vulnerability evaluations and testing by skilled security specialists are critical components for the same. These proactive techniques, serves as a security lens, detecting exploitable flaws or Loopholes in methods before the hacker may strike. Additionally, introducing realistic security measures like, multi-factor authentication improves the overall safety stance of the organization. By combining with regular staff instruction on cyber guidelines, these approaches instigate employees to take an active role in organisational cyber defence. Organisations may measurably improve their cyber resilience and limit the risks presented by changing cybercrime threats by developing an atmosphere of security awareness and prioritising certain protective steps. The regular risk assessment, precise safety measures, immediate plans for responding the hazards, co operations, system updates etc. can help in safeguarding the organizations private data from cyber hazards.

VII. RESEARCH METHODOLOGY

The research methodology adopted in this paper is purely doctrinal in nature. Doctrinal research, also known as library-based research, is a distinctive method of

conducting legal research that involves the study and analysis of existing legal provisions, case laws, and scholarly works. This methodology is well-suited for examining the theoretical and conceptual aspects of law and for providing a systematic exposition of legal doctrines and principles. The primary sources relied upon in doctrinal research include statutory materials, judicial precedents, and authoritative texts, while secondary sources such as commentaries, articles and legal digests are also consulted. The research process involves the identification, collection, and critical analysis of these sources to draw logical conclusions and offer insights into the legal issues under investigation. Through doctrinal research, this paper seeks to provide a comprehensive and coherent understanding of the legal framework governing the subject matter at hand.

VIII. LITERATURE REVIEW

This research paper draws attention towards the IT Act,2000 along with it comparing the provisions given under Constitution of India, Indian Penal Code, 1860 etc. along with certain guidelines which are imposed by RBI and some statutes which are about to came into force in the near future. This paper also throws lights on various landmark judgement which were given by the Apex Court of India I.e. ***Shreya Singhal vs UOI, CBI vs Arif Azim, SMC Pneumatics (India) Pvt. Ltd. vs. Jogesh Kwatra*** *etc.* These case laws help to reduce the differentiations which generally arise when there is a question about the applicability of specific provisions and common laws.

The literature reviewed in this paper provides brief knowledge about the gravity of cyber frauds and provisions which are there to prevent the damage of general people. It also gives significant practical case studies which helps to understand the real-life impacts of this cybercrimes in depth and ways to stay away to trap in these frauds.

IX. MEANING, DEFINITION & EXPLANATION

Cybercrime involves a wide range of unlawful crimes carried out via digital methods. Such as computer hacking, phishing, virus assaults, and online scamming. Hackers use technology flaws to obtain important information, interrupt business processes,

or extract funds. The advancement of technology has assisted this unlawful behaviour, allowing offenders to conduct business secretly throughout countries. As our reliance on technology rises, combatting cybercrime continues a key concern for administrators, businesses, and citizens.

The definition which is mentioned under the statute specifies that any action of damaging, changing, or hacking a computer system/network or erasing information by hazardous motive without the permission of the authority of the system is subject to monetary payment as compensation for losses.[2]

Cybercrime is "offences conducted contrary to individuals or group of people having an unlawful intention to deliberately damage the image of the person being targeted or create harm, whether physical or mental, or damage, to the sufferer either directly or through indirect means via modern networks for telecommunication like the World Wide Web."[3]

The term "cybercrime" refers to "illicit offences contrary to individuals through computer equipment and connections, especially the unlawful use of creator's rights."[4] According to Pawan Duggal, "Cybercrime means to all unlawful conduct carried out in cyberspace or via the use of the internet." These might be traditional criminal acts or behaviours that have emerged as a result of the new medium's development. Cybercrime encompasses any behaviour that offends public abilities.

X. HISTORICAL BACKGROUND / EVOLUTION OF CYBERCRIME IN INDIA

India saw an explosion in cyber fraud during the initial times of 2000. This explosion was nothing but mushrooming of the cyber fraud and scams. This scam includes various types of fraud within it such as, phishing attacks, e-lottery scams, fraud involving advance payments etc. As these kinds of events started growing continuously it required a lot of awareness and strong enforcement of actions against it all across the country. By acknowledging the severity of this incidents, various

[2] Information and technology act, 2000
[3] United Nations Office on Drugs and Crime (UNODC)
[4] Definition by Council Of Europe

organizations started to accentuate the requirement of cyber security education and awareness programs and also enforced measures for combating this growing risk. All these instances were a watershed point of the history of Indian cyber security journey. Which forced to establish legislation for implementing various rules and policies which will target towards improving cyber resilience and will help to protect digital eco system.

As we know need is the ultimate mother of innovation. Similarly, there was a requirement of specific legislation to protect digital eco system in India which gave birth to INFORMATION AND TECNOLOGY ACT, 2000[5]. This act provides legal legitimacy to digital transactions as well as addresses the problems of digital crime which are associated with it. It also defines numerous varieties of cyber-crime and provide frameworks for the same. After the act came into force, various units of cyber cell were instituted in several states of India for tackling the rapid growth of cybercrime. In the year 2008, the existing act was amended to reinforce cyber fraud laws and broadens the scope of this crime. This modification includes various clauses like safeguarding of the information, confidentiality of individuals, digital signing etc. this amendment also increased the level of penalties for the same.

India has initiated end number of programmes and collaborative efforts to boost the cyber security and to prevent cyber-crimes. It also established National agencies to respond cybercrimes immediately by collaborating with foreign events such as GCI (Global Cyber security Index).

Over the past few years, India has experienced prominent instances of Cybercrimes which encompasses a variety of offences. One of those incidents was "ICICI BANK LTD v. M. UMASHANKAR SIVASUBRAMANIAN"[6] which is known as first ever phishing case of India. And the court by giving the decision of this case ordered the bank to pay compensation amount.

The prolonged background of cybercrime in history of India illustrates the ever-changing nature of modern technology as well as the issues which are associated with

[5] Information and Technology Act, 2000
[6] CMA.2863/2019

the same. The law makers, the enforcement authorities of law, and the stake holders of the cyber security are still working to improve the legislative frameworks of cyber-crime to execute strong measures to combat th same in the country.

XI. TYPES OF CYBER-CRIME IN BUSINESS

In today's corporate environment, the intricacy interplay of the organizations helps to being the excellent target of cyber-criminals. These digital assaults are not only interrupting the business but also cause to major harm to the organization in case of financial as well as reputational. These digital criminals generally make use of a larger variety of cyber-crimes to carry out those harmful campaigns. These types of campaigns are carried out for financial gain only by conducting malicious intentions. The followings are the most prevalent types of cyber-crime which targets at the organizations.

A. Data Breaches

Data breaches is the widest aspect of cyber-crime. All form of cyber-crime is associated with data breaches. Simply, data breaches means when the confidentiality of the data of the person/organizations is breached or compromised. Whenever an unauthorized person gets the accessibility to the confidential data and information through wrongful ways, and steals those corporate data, this leads to data breaches. Those confidential data include different types of information's like record of the consumers, information's related to finances of the organizations, different intellectual properties, business correspondences etc.

1. **Aadhar data breach case (October 2023):** This recent case is known as the biggest data breach case in the history of Indian cyber security. In this case individual data of more than 81.5cr was leaked. It has been alleged that all those person and confidential information of many people was leaked from the Indian Council of Media Research website.[7]

[7] Aadhaar details of 81.5 cr people leaked in India's 'biggest' data breach - Hindustan Times, https://www.hindustantimes.com/technology/in-indias-biggest-data-breach-personal-information-of-81-5-crore-people-leaked-101698719306335.html.

2. **AIR India data breach case (May 2021):** A cyber-attack on the system of AIR India had taken place on May 2021 which led to leaking of personal data of so many passengers. This has been done from the site of SITA which is the Airline data service provider.[8]

B. Phishing Attacks

Phishing attacks are the deceptive operations in which the attacker impersonates a legitimate company or person using email, instant messaging and other communication methods. In this the attacker generally uses misleading messages to make fool to the general public/corporations for disclosing those confidential data Infront of them.

A phishing assault can be designed to collect sensitive information or data for nefarious reasons by installing malware on the device of the victim or to abuse the person in other different ways.

1. **State Bank of India Phishing attack case:** It is one of the most noteworthy case of phishing attack which was occurred in the year of 2018. In this case the cyber criminals were targeting the customers of SBI. They used to send fake emails to customers by appearing themselves as a person from bank and were asking them to update their personal and financial details into one online portal which was appearing as SBI portal. This case gained a lot of attention as it raised question about the cyber security of the bank as well as about the confidentiality of the private information's of the customers. [9]

C. Ransomware-

This is a sort of a malicious software which is also known as malware. It threatens to publish or block the access of a computer device by encrypting the same. The hacker threatens the person to pay a ransom amount of money to prevent from it. This attack can take various forms like, encrypting ransomware, screen locking ransomware in

[8] The biggest data breaches in India | CSO Online, https://www.csoonline.com/article/569325/the-biggest-data-breaches-in-india.html.
[9] Phishing Scam: SBI account holders, State Bank of India never sends these messages; warns the government - Times of India, https://timesofindia.indiatimes.com/gadgets-news/sms-asking-users-to-update-their-pan-card-to-avoid-their-account-getting-blocked-is-a-scam-pib-fact-check/articleshow/106000916.cms.

which the hacker locks the scree of the individuals by displaying a particular screen which demands to pay certain amount. Leak ware or do ware which threatens the individual to broadcast the sensitive information's, in case he fails to pay. These are only few types of cyber fraud that takes place frequently in the society. Except these there are end number of cyber frauds which comes within the broader ambit of this. They are social engineering, crypto jacking, supply chain attacks, etc.

XII. DEFENCES AGAINST CYBER CRIME

Now a days cybercrime is becoming a steadily growing serious issue which needs proper framework and complete plan to defence. Network security is on of the critical security which includes firewalls, intrusion detection system, network segmentation etc. similarly end point security is also providing a strong protection by including powerful anti-virus and anti-malware software within its ambit. Data security encompasses implementation of strict actions by encrypting sensitive information's. Employee training in data protection also plays a crucial role to identify and address those crucial problems. Patch management guarantees that the security fixers are deployed in a timely manner. Back-ups of those critical data facilitate the rapid recovery of data in case of a cyber-attack. Business strategies should be made to tackle such cyberattacks. After taking these preventive measures another important measure is to make cyber insurance. Which will assist to offset all the expenditures which will occur due to cyberattacks.

XIII. LEGAL PROVISIONS / PROCEDURE / SPECIFICATIONS / CRITERIA

The specific statute which prevents the Individual and organizations against the cyber offences is Information and technology act, 2000. Other than this, there are certain provisions mentioned under Indian Penal Code (IPC) which can be added along with IT provisions.

Different sections of IT act deals with different types of cyberattacks. Section 43 of the act deals with data breaches whereas section 65 of the same code deals with those strategies which are made to steal data from the devices. Similarly, section 66 of the

Act is the combination of other types of cyberfraud but in a broader sense. The provisions under this section have been inserted after the amendment act.

Specifically, section 463,465, and 469 of IPC are associated with the punishment and provisions for cybercrimes. In business sector, other than the provisions of IT ACT,2000, and IPC,1860, there are other statutes which deals with cyber frauds. They are, RBI Guidelines; it issues specific guidelines to ensure specific security measure in banking sectors. These guidelines of RBI are mandatorily applicable in the banking and financial institutes. Data protection law; the new statute which is going to come up super soon is underworking. This particular act will have specific significant impacts on those personal data which are used to handle the businesses.

XIV. CASE LAWS / PRECEDENTS / OVERRULING

Followings are certain landmark cases of cybercrime in India**.**

A. Shreya Singhal v. Union of India[10]

This is one of most leading yet widely popular case of cyber-crime in India. In this case two ladies were arrested under section 66A of Information and technology act,2000 as they posted abusive and inappropriate remarks about the full closure of Mumbai which was held due to the death of a politician, in the Facebook. In defence, these 2 ladies filed a defence by challenging the validity of section 66A by stating that this particular provision violates the right to freedom of speech and expression which has been given under Article 19 of Constitution of India.

Validity of Section 66A of IT Act,2000 was challenged before the Supreme court of India. While giving the judgement the court held that, the decision of the case regarding this particular matter will be based on 3 concepts. They are discussion, advocacy and incitement. The Apex court observed that, mere discussion as well advocacy of any specific topic is the heart and soul of the concept freedom of speech and expression under Article 19 of Indian Constitution although it is not widely accepted. Supreme court also stated that section 66A of IT Act can restrict every type

[10] AIR 2015 SC 1523

of communication and it encompasses no differentiation between advocacy or discussion on any offence matter.

The court held that, section 66A is not safeguarded on the virtue of being a reasonable restriction which should be applied in case of freedom of speech and expression. And the case dismissed on this ground.

B. CBI v. Arif Azim[11]

This is another landmark case on cyber law and widely known as SONYSAMBADH case. In this case there was a website known as sonysambandh.com which was providing Sony products to NRIs to send it to their Indian friends and relatives after an online payment. Once someone logged into the website and ordered one colour TV set for the defendant who was living in Noida. While doing the online transaction the credit card authority informed the person that this is an unauthorized transaction as the original owner refused to accept such purchase. After this incident, a case filed with CBI and after case has been filed in the court. During investigation it has been uncovered that the defendant was using the credit credentials of the purchaser wrongfully when she was not using the same.

As the judgement, the court held the defendant as liable and convicted him for one year. This case is the water washed which shows that except the provisions of IT act there are certain provisions which are mentioned under IPC to rely on.

C. SMC Pneumatics (India) Pvt. Ltd. v. Jogesh Kwatra [12]

In this case the defendant was the employee of the plaintiff's company. He was sending all diminishing, defamatory, filthy and abusive emails to defame the company to all its employee not only in the main branch but also in the subsidiary branches of the same. In the investigation it has been found that the emails are generated from one of the cybercafe of New Delhi by the defendant. It was held in the case that the suit has been dismissed, as there is no direct and sufficient evidence to prove the allegation. The court also directed to the defendant to not publish any kind

[11] (2008) 150 DLT 769
[12] CM APPL. No. 33474 of 2016

of information regarding to the company or its owner which is defamatory and abusive as well as derogatory in nature.

XV. CONCLUSION, SUGGESTIONS & RECOMMENDATIONS

Cyber law is a growing yet severe problem in today's world which is so severe to destroy anyone's personal and credential information in just seconds. For overcoming this ever-evolving problem people need to be aware as well as educated about the preventive steps and provisions which are related to these crimes. By understanding and applying these preventive methods and rules into daily life while doing any kind of transaction online, a person can be saved from the evil eyes of these hackers.

For decreasing the graph of this cyber-fraud government needs to impose strict provisions and security for the same. Only by establishing these measurements and tightening the punishment this problem will be solved. This research paper tries to shed lights on the digital footprints of the cyber-fraud in the field of corporate while investigating various types of cyber threats and the consequences of the same. In a world that is becoming more interconnected, organisations may improve their safety measures and secure their digital possessions by deploying successful mitigation methods and remaining a step ahead of new hazards.

XVI. REFERENCES

A. Online Articles / Sources Referred

1. Aadhaar details of 81.5 cr people leaked in India's 'biggest' data breach - Hindustan Times, https://www.hindustantimes.com/technology/in-indias-biggest-data-breach-personal-information-of-81-5-crore-people-leaked-101698719306335.html.
2. The biggest data breaches in India | CSO Online, https://www.csoonline.com/article/569325/the-biggest-data-breaches-in-india.html.
3. Phishing Scam: SBI account holders, State Bank of India never sends these messages; warns the government - Times of India, https://timesofindia.indiatimes.com/gadgets-news/sms-asking-users-to-

update-their-pan-card-to-avoid-their-account-getting-blocked-is-a-scam-pib-fact-check/articleshow/106000916.cms.

4. https://enhelion.com/blogs/2021/03/01/landmark-cyber-law-cases-in-india/#_ftn9
5. https://arcticwolf.com/resources/blog/decade-of-cybercrime/
6. https://www.researchgate.net/publication/334124155_Cyber_Crime_Scenario_in_India_and_Judicial_Response
7. https://www.stickmancyber.com/cybersecurity-blog/impact-of-cybercrime-on-business-cybercrime-business-continuity

B. Cases Referred

1. "ICICI BANK LTD v. M. UMASHANKAR SIVASUBRAMANIAN" CMA.2863/2019
2. Aadhar data breach case (October 2023)
3. AIR India data breach case (May 2021)
4. State Bank of India Phishing attack case
5. Shreya Singhal vs Union of India AIR 2015 SC 1523
6. CBI vs Arif Azim (2008) 150 DLT 769
7. SMC Pneumatics (India) Pvt. Ltd. vs. Jogesh Kwatra CM APPL. No. 33474 of 2016

C. Statutes Referred

1. Information and Technology act,2000
2. Indian Penal Code,1860
3. Constitution of India
4. Data protection Law