International Journal of Science and Research (IJSR)
ISSN: 2319-7064
Impact Factor 2024: 7.101

Cyber Fraud in the Digital Age: Case Studies, Legal Challenges, and the Need for Robust Data Protection

Megha Kavtiyal

Student Uttaranchal University, Dehradun, India

Abstract: ***The escalating tide of cybercrime represents not merely a technological failure, but a deeply embedded human and procedural vulnerability in today's digital framework. This article brings into sharp focus how cyberspace, while immensely beneficial for communication and commerce, has simultaneously opened the floodgates to sophisticated online crimes. By analyzing prominent global cases like the Sony Pictures hack, India's first cybercrime conviction through sony.sambandh.com, and the high-profile phishing scam involving Nidhi Razdan, the study exposes the evolving nature of cyber threats—now often seen as structured, professional careers rather than sporadic acts of mischief. It is evident that the anonymity offered by the internet has emboldened perpetrators, making tracking and prosecution an uphill battle. This work also reflects on the unique challenges faced by developing nations like Zimbabwe, where outdated systems could ironically provide temporary insulation against such attacks, yet hinder recovery if targeted. The discussion on legal loopholes, especially in the context of data privacy laws, paints a picture of a regulatory ecosystem struggling to keep up with cyber threats. What stands out is the tension between privacy and security, with the article suggesting pragmatic solutions like "regulated pseudonymity" as a bridge between the two. Overall, the narrative not only explores the anatomy of cybercrimes but also underlines the pressing need for adaptive laws, better corporate defense mechanisms, and public awareness to stem the rising tide.***

Keywords: Cybercrime evolution, data privacy law, phishing scams, cyber-attack case studies, digital security awareness

1. Introduction

The chapter begins with the words of Ginni Rometty, former CEO of IBM, who rightly said, *"Cybercrime is the greatest threat to every company in the world."* Her statement highlights the growing risk that cybercrimes pose to businesses across the globe. Stating which it won't be wrong to state that cyberspace is gaining greater attention these days as its reach expands into practically every facet of our life. It has become a prominent topic of discussion among the media and different public and private sector organizations. Its negative consequences are frequently emphasized in the news and media. Because practically everyone uses cyberspace and its services, whether directly or indirectly, it is critical for everyone to understand its scope, breadth, and potentially fatal consequences. People's awareness of cyber security is now critical in order to mitigate its negative consequences. In actuality, cyber security is not a new concern; the same issue existed in a different scenario before a decade. Cybercrimes is a strategic problem, a human problem, and a process problem, not a technological one. Cyber-attacks were not as dangerous as they are now. The number of cyber-attacks was quite low. At first, cyber-attacks were used to make people frightened. The goal was not to make money, but the situation has changed, and internet has now been transformed into a safe tool for counterfeiting and criminal activity. On the one hand, cyberspace is regarded as advantageous since it gives information and services in a very short time and at a relatively low cost all over the world. It, on the other hand, has the disadvantage of being vulnerable to cyber-attacks. As it is borderless, it can be found in every corner of the globe. Nature is shapeless. It is becoming increasingly difficult to apprehend cybercriminals. As it gets more difficult to spot guilty people, they become criminals almost instantaneously, because of the actor's anonymity in cyberspace.

It is one of the characteristics of the internet that allows it to grow swiftly and sustainably. It is accessible to all end users and innovators for both creation and governance. These two are, Access issues do not occur in isolation, but rather as a result of a combination of factors. The same virtual environment. In the last two decades, cyberspace has grown significantly. Terrorists benefited from the internet and cyberspace as well.

Cybercrime is one industry that has experienced double-digit growth in recent years of economic expansion. Cybercrime is now considered a legitimate career. In early 1990s, when cybercrime began to appear in the form of males between the ages of 20 and 30 years were involved in hackings. It was all for the sake of having a good time. With the date, the age group, the goal, and the scope of the cybercrime. The face of crime has shifted tremendously. In today's internet world. Criminals of any age can be found. They've accepted it as their own profession. It is seen as a source of revenue. As a consequence, Cyber-attack are becoming increasingly sophisticated. Another factor contributing to the rise of cybercrime is ready-made harmful software. This programme is available for purchase and can be used to steal credit card numbers and other sensitive information.

2. Analysis of Sony Hack

Sony pictures entertainment and North Korea Sony Pictures Entertainment is a firm that provides entertainment and assists with media distribution across the world. North Korea is the most divisive leader in the world. This means

that Sony, as an entertainment firm, has its own databases. North Korea is a threat since it was involved in the assault in some way. A large amount of sensitive information was exposed, including:

- Unreleased films
- usernames and passwords for Sony employees
- sensitive information regarding the company's network architecture
- a slew of papers revealing personal information about employees
- emails from business partners

When and How it Occurred

Sony Pictures Entertainment chose Christmas Day 2014 to release the picture in cinemas. An email sent to Sony Pictures CEO Michael Lynton, Chairman Amy Pascal, and senior officials on November 21, 2014 made vague references to "grave damage" and requested "monetary compensation" to avert it. On November 24, 2014, a Reddit article claimed that Sony Pictures Entertainment had been hacked and that their whole internal, national network contained indicators that the attack had been carried out by a group known as the GOP, The Guardians of Peace. The FBI sent a classified notice to a number of U.S. companies, warning them that hackers had just launched a destructive "wiper" cyber-attack. The hackers claim to have stolen a massive amount of sensitive information from Sony, maybe up to 100 gigabytes, which they are progressively publishing in batches.

Effects of the Incident

The hackers posted identities, passwords, and critical information about Sony's network architecture, as well as a slew of papers disclosing personal information about workers, personal emails from business partners, and unreleased films, on the internet. As a result, the company's personnel were open to assaults, and millions of dollars were stolen.

Overall Impact

The majority of the consumers that were impacted were left susceptible to ransom ware assaults. Employees were the most affected, as the majority of their personal information, such as salary and home addresses, was made public. The corporation suffered significant financial losses as a result of the leaked unreleased films. Emails from several partners that were hacked revealed a great deal of personal information about their partners, prompting many to terminate their contracts with Sony. In a wide-ranging interview, Lynton, Sony's CEO, addressed to the attack's isolation and uncertainty, as well as the unusual position the firm found itself in, saying that "there's no blueprint for an occurrence like this," which made Sony's recovery more difficult. While Sony indicated in an earnings report that the breach would cost the company $15 million in "investigation and remediation charges" for the quarter ending December 31, senior general manager Kazuhiko Takeda stated that the company would lose $35 million for the fiscal year ending March.

The Impact with Respect to Zimbabwe

If such an incident occurred in a Zimbabwean company, such as the ZBC ("Zimbabwe Broadcasting Company"), it would have a negative impact because there is little or no assurance that the company will recover from the incident due to poor technologies or a lack of knowledge on how to respond to such attacks. However, because Zimbabwe is a developing country, the attack would reveal certain facts about the company's future objectives.

Probability of Occurrence

The probability of such an incident happening in Zimbabwe is very low basing on the economic status of the country and the technologies being used by most companies that is they are still using written records to store their information and most of their databases are still using offline protocols due to poor or little technologies being used. The probability of such an incident happening in Zimbabwe is very low basing on the economic status of the country and the technologies being used by most companies that is they are still using written records to store their information and most of their databases are still using offline protocols due to poor or little technologies being used. The likelihood of such an incident occurring in Zimbabwe is extremely low, given the country's economic situation and the technologies employed by most businesses, which include the use of written records to store information and the use of offline protocols in most databases due to poor or limited technology.

SWOT Analysis

Strength

a) Sony, as a large corporation, had financial benefits since it could weather periods of unprofitability.
b) They continued to offer services long after the assault, producing films.

Weaknesses

a) Inadequate malware protection at Sony Pictures Entertainment.
b) They had poor incident response systems
c) poor defense mechanisms because a similar incident had occurred previously and they had not yet learned from it
d) They had poor monitoring, audit logs, encryption, and controlled use of administrative credentials because a similar incident had occurred previously and they had not yet learned from it.

Opportunities

a) Loss of client confidentiality
b) Sony may plan more strategically to compensate for lost income, as it does with other areas of business.

SONY.SAMBANDH.COM CASE

In 2013, India received its first cybercrime conviction. It all started when Sony India Private Ltd, which controls the website www.sony-sambandh.com and targets Non-Resident Indians, filed a complaint. NRIs may use the service to transfer Sony items to friends and family in India after paying for them online. The firm guarantees that the items will be delivered to the intended recipients. According to the cybercrime case study, in May 2002, someone using the name Barbara Campa went onto the website and bought a Sony Color Television and a cordless headphone. She

provided her credit card information and asked for the items to be sent to Arif Azim in Noida. The credit card company cleared the payment, and the transaction was completed. The products were delivered to Arif Azim after the business completed the necessary due diligence and inspection processes. The firm took digital images of Arif Azim accepting the item at the time of delivery. The transaction was completed at that point, but after one and a half months, the credit card company alerted the firm that the purchase was unlawful since the genuine owner had denied making it. The firm reported internet cheating to the Central Bureau of Investigation, which opened an investigation under *Indian Penal Code Sections* ***418, 419, and 420*****.** Arif Azim was detained once the case was examined. Arif Azim obtained the credit card number of an American national while working at a contact centre in Noida, which he exploited on the company's website, according to investigations. In this one-of-a-kind cyber fraud case, the CBI retrieved the color television and cordless headphone. The CBI had enough evidence to establish their case in this instance, thus the accused accepted his guilt. Arif Azim was found guilty under Sections 418, 419, and 420 of the Indian Penal Code, marking the first time that cybercrime has been found guilty.

Judgement

The court, on the other hand, believed that because the accused was a young kid of 24 years old and a first-time offender, a liberal approach was required. As a result, the court sentenced the accused to a year of probation. The decision has enormous ramifications for the entire country. Apart from being the first cybercrime conviction, it has demonstrated that the Indian Penal Code may be effectively used to some types of cybercrime that are not covered under the Information Technology Act 2000. Second, a decision like this sends a strong message to everyone that the law cannot be manipulated.

Nidhi Razdan Phising Attack

In a phishing assault, a former NDTV anchor was supposedly given a teaching post at Harvard University's college of arts and sciences, which does not have a department of journalism. After a careful review of its people-related systems, Harvard is understood to have found no record of, nor any knowledge of, an appointment involving the former TV news anchor, Nidhi Razdan. Razdan has said in a statement she accepted a job offer for the position of associate professor of journalism at Harvard University in 2020, but she began noticing a number of ―administrative anomalies after her joining date was shifted from September 2020 to January 2021, ostensibly because of the Covid-19 pandemic. Harvard is one of the few US institutions of higher learning to have switched entirely to online teaching because of the pandemic, which hit this country the hardest. Many other institutions have opted for a hybrid model of online and in-person teaching

In her statement, Razdan did not specify which Harvard school or faculty member offered her the alleged offer. The Faculty of Arts and Sciences at Harvard University does not have a journalism department. In truth, the university lacks a professional journalism school. Names listed as members of human resources in the materials given by Razdan were not located on Harvard's personnel lists, and a number of inconsistencies in the agreement document, which would have formalized the bogus employment offer, are said to have been discovered by Harvard. For **one thing,** Harvard faculty appointments are not assessed, as Razdan's records, which were shared with the institution, suggest. **Second,** several of the agreement's restrictions do not apply to Harvard faculty members. It was impossible to tell what the supplies were right away. **Third,** and lastly, two of the claimed signatories of the agreement are believed to have indicated that they did not execute the attached agreement.

An Analysis

Some parts of the data protection legislation require a closer examination to see how they apply to this sort of cybercrime. "Privacy" is frequently used to conceal information. As a result, under the pretense of "privacy," a website's "Who Is" data is not made widely available, and the originating IP address in emails is obscured. These factors directly contribute to email impersonation. At the same time, there are parts of law enforcement who try to fix investigations by abusing legal powers. When such misuse happens, many experts keep silent, and as a result, the problem persists. This has fostered a schism between society and law enforcement, and any suggestion that they should be granted investigative powers under the data privacy laws is unwelcome. It is this distrust that makes it difficult to arrive at a data protection law that provides enough flexibility to investigators without them misusing the powers. Finding the right balance may even be impossible in the current structure of law enforcement unless we create a layer of intermediary service providers who provide ―regulated pseudonymity. This can assist data principals in protecting their privacy, enable business to pursue their legitimate interests and allow law enforcement to get appropriate information to help their investigations with a check on the misuse. Fortunately, the Indian Personal Data Protection Bill 2019 provides for such a mechanism and if properly harnessed, we will be able to find a balance between privacy and security, which is eluding us for a long time. We should also remember that one of the privacy protections measures that GDPR and now PDPB 2019 suggest is that personal data should be periodically updated to maintain accuracy. This requires the service provider to ask for updation from time to time which itself can be a possible source of phishing.

[1]This mistrust makes it difficult to come up with a data protection regulation that gives investigators adequate leeway without allowing them to abuse their authority. In the existing system of law enforcement, finding the correct balance may be impossible unless we build a layer of intermediate service providers who provide "controlled pseudonymity." This can help data owners preserve their privacy, businesses pursue their legitimate interests, and law enforcement receive the information they need to aid them with their investigations while keeping a lid on the misuse.

3. Suggestions

People lose millions every year to online fraud, but there are some precautions and measures one can take to avoid falling victim to such schemes.

- Set strong password
- Keep your device updated
- Beware of phishing
- Secure Wi-Fi
- Keep your data personal
- Check website authenticity

4. Recommendations

- Automatically block malicious E-mail by implementing Spam detectors which can help to keep the consumer from ever opening the suspicious email.
- Automatically detect and delete malicious software and spyware by installing any of specialized commercial programs.
- Education remains critical so that people are aware of both the phishing techniques and how legitimate entities will communicate with them via E-mail and the web.

5. Conclusion

It is incredibly difficult to be certain of a person's involvement in a cybercrime. It's also tough to track out the source of cybercrime. Because of these aforementioned factors, the rate of cybercrime is rapidly increasing. In this paper, we will look upon. We've gone through the basics of cyberspace and how it works. *Why do crooks use the internet as a fantastic tool? A tool for committing crimes?* Following that, we have the numerous regions where identity theft is occurring abused to commit fraud Theft rates for various products are detailed in the international black market for cyberspace. The study also discusses the numerous driving reasons that led to the decision. Personal information that is frequently used as a target in a variety of situations in cybercrime. Cyber fraudsters do not even have to leave their homes to commit fraud, as they can route communications through local phone companies, long - distance carriers, Internet service providers, and wireless and satellite networks. To prevent the increasingly numerous frauds spawned by the information age, management must know its vulnerabilities and be able to mitigate risk in a cost - effective manner. Therefore, IT risk should be directly included in the organization' s overall fraud risk assessment and resulting preventive controls.

References

[1] The Information Technology Act, No. 21 of 2000, § 43, INDIA CODE (2000), https://legislative.gov.in/actsofparliamentfromtheyear/information-technology-act-2000.
[2] Indian Penal Code, No. 45 of 1860, §§ 418, 419, 420, INDIA CODE (1860), https://indiacode.nic.in/.
[3] The Personal Data Protection Bill, Bill No. 373 of 2019, PRS LEGISLATIVE RESEARCH (India), https://prsindia.org/billtrack/personal-data-protection-bill-2019.
[4] Regulation (EU) 2016/679, General Data Protection Regulation, 2016 O.J. (L 119) 1, https://gdpr-info.eu/.
[5] Ministry of Electronics and Information Technology, National Cyber Security Policy 2013, MEITY (India), https://www.meity.gov.in/writereaddata/files/National_cyber_security_policy-2013%281%29.pdf.
[6] Press Release, FBI, Update on Sony Investigation (Dec. 19, 2014), https://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation.
[7] CBI, Cyber Crime Conviction Report: Sony Sambandh Case (2002), https://cbi.gov.in/.
[8] Nidhi Razdan, *Phishing Scam: My Experience of a Fake Harvard Job Offer*, THE WIRE (Jan. 15, 2021), https://thewire.in/media/nidhi-razdan-harvard-phishing-scam.
[9] Symantec Corp., Internet Security Threat Report, Vol. 23 (2018), https://www.symantec.com/security-center/threat-report.
[10] Verizon, Data Breach Investigations Report (2023), https://www.verizon.com/business/resources/reports/dbir/.
[11] *Cybercrime and Cybersecurity in India: Legal Challenges and Remedies*, 8 NUJS L. REV. 1 (2015), https://nujslawreview.org/.
[12] M. Krishnamurthy, *Cybersecurity and the Law in India*, 9 J. CYBER L. (2020) (India), available at Manupatra.
[13] N. Bhatia, *Digital Crime: Cyber Fraud and Data Theft in India*, 48 INDIAN J. CRIMINOLOGY (2021), available at JSTOR.
[14] INTERPOL, Cybercrime Annual Report (2022), https://www.interpol.int/en/Crimes/Cybercrime.
[15] World Economic Forum, Global Cybersecurity Outlook 2023, https://www.weforum.org/reports/global-cybersecurity-outlook-2023.
[16] UNODC, Comprehensive Study on Cybercrime (2013), UNITED NATIONS OFFICE ON DRUGS AND CRIME, https://www.unodc.org/unodc/en/cybercrime/.
[17] Microsoft, Digital Defense Report 2023, https://www.microsoft.com/en-us/security/blog/microsoft-digital-defense-report/.
[18] CERT-In, Annual Reports, INDIAN COMPUTER EMERGENCY RESPONSE TEAM, https://www.cert-in.org.in/.
[19] Sony Hack: FBI Blames North Korea, BBC NEWS (Dec. 20, 2014), https://www.bbc.com/news/entertainment-arts-30512032.
[20] India Sees 18 Million Cyberattacks in Q1 of 2022, ECON. TIMES (Apr. 4, 2022), https://economictimes.indiatimes.com/.