WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Cybercrime in The E-Commerce Era: Challenges, Risks, and Solutions in India

Isha

Maharishi Markandeshwar Deemed to be University, Mullana

DOI : https://doi.org/10.55248/gengpi.6.0325.12183

ABSTRACT

The majority of commercial transactions involving the purchase and shipment of products and services take place inside the realm of electronic commerce, or E-Commerce. As electronic commerce relies on the Internet to do business, it's important to be aware of the factors that can undermine consumer confidence in this sector, such as cybercrime.

The use of sophisticated computer networks for illegal purposes, such as launching denial-of-service attacks, phishing, hacking, or damaging victims' reputations or stealing information, is known as cybercrime, e-crime, electronic crime, hi-tech crime, or computer crime.

This paper discusses prevalence and nature of cybercrime in India with respect to E commerce industry and also delves into the key challenges faced by e-commerce businesses in India regarding cybersecurity. The paper also discusses various cybersecurity measures in India in combating e-commerce-related cybercrime.

Keywords- *E commerce, cybercrime, computer, phishing, hacking and etc.*

1. INTRODUCTION

The proliferation of e-commerce platforms has created new entry points for cybercriminals. Internet users throughout the world are constantly developing, which is leading to a growth in e-commerce technology and the transactions that go along with them. The number of people using the Internet is expected to reach 3 billion by 2015, up from 361 million in 2000 and 1.97 billion in 2020. The number of people using the Internet has been steadily rising for some time. By 2029, the number of internet users in India would have surpassed 10 million, up from 2 million in 2019.[1]

It is essential that all parties involved in an online transaction feel secure. It is well recognized that trust plays a crucial role in conducting commercial transactions online. Because the Internet is accessible to everyone, it has become a platform for cybercrime. Cybercriminals' ability to remain anonymous online makes it all the more difficult to uncover their true motives and put an end to their criminal acts.

All things considered, failing to implement adequate security measures makes online business transactions very risky for everyone involved. In order to commit crimes, some people are too careless with their online activities, and cybercriminals take advantage of security holes in computer networks and the internet itself. [2]

1.1 Research Questions

1. How does the increase in screen time and e-commerce activities impact the prevalence and nature of cybercrime in India?
2. What are the key challenges faced by e-commerce businesses in India regarding cybersecurity, and how do these challenges affect consumer trust and business operations?
3. How effective are current regulatory frameworks and cybersecurity measures in India in combating e-commerce-related cybercrime, and what improvements can be made?

[1] Dueep J. Singh, *Introduction to Internet Scams and Fraud - Credit Card Theft, Work-At-Home Scams and Lottery Scams* 46-57 (Mendon Cottage Books, 2015).
[2] Rohan Nagpal, "Offences and penalties under the Information Technology Act, 2000" 8 *Information Technology Law Journal* 18-45 (2002).

1.2 Statement of Problem

When a firm falls prey to cybercrime, its reputation tarnishes because its customers start doing business with competitors. People may lose faith in a company's capacity to protect their personal information and efficiently handle sales transactions if they see that it is susceptible to cybercrime. Therefore, in order to protect themselves against Cyber Crime, businesses must fight. Not only does cybercrime cost businesses money, but it also drives consumers away. However, it undermines the confidence of online merchants and shoppers alike.

1.3 Research Methodology

The methodology used in the paper is doctrinal in nature. The researched has gathered information from both primary and secondary sources like statutes, case laws, commentaries, reports, books, journal articles and websites.

2. CONVENIENCE AND CYBERCRIME IN INDIA'S DIGITAL MARKET

2.1 The Impact of Online Time on E-commerce Growth and Cybercrime

The growth of e-commerce is influenced by the amount of time people spend online. The term "e-commerce" refers to the practice of selling, purchasing, transferring, and exchanging goods and services via the use of electronic devices and the Internet. The proliferation of e-commerce models is largely attributable to the expansion of the Internet.

Companies see e-commerce as a game-changer that can improve their operations in many ways. Worldwide, online shopping has surpassed more conventional and time-consuming methods of doing business on a global scale. The expansion of e-commerce technologies has been driven mostly by the rapid use of the Internet and powerful mobile devices, together with remarkable advancements in technology.[3]

Among the many benefits of doing business online are the following: the ability to trade at any hour of the day or night, a significant competitive advantage, mass personalization, a decrease in operational costs, and access to foreign marketplaces. Businesses may reap the benefits of time and money savings via e-commerce. Consequently, companies benefit from e-commerce since it boosts financial performance and makes corporate operations more productive.

Cybercrime and other forms of online crime are becoming more common on a global scale. The lack of a proper legal framework to address cybercriminals has contributed to the proliferation of cybercrime. Possible explanation: differing opinions on punishing cybercriminals.

For fear of public distrust and reputational harm, many organizations and individuals are hesitant to disclose cybercrime incidents to the proper authorities. Foreigners are the most common victims of fraud in these situations. Online shoppers are understandably wary of making purchases via e-commerce platforms due to the prevalence of cybercrimes in the industry.[4]

2.2 Understanding the Threats in the Digital Marketplace

Online and mobile commerce have replaced traditional brick-and-mortar stores as the new norm, allowing consumers to buy and sell whenever and wherever they choose with the tap of a finger. One of the greatest benefits of e-commerce is the convenience it brings to both buying and making financial transactions. The convenience of internet banking has led to all banks establishing desktop and smartphone forms.[5]

Cybercriminals target businesses that deal in the transfer of money and personal information. Without considering the potential dangers of the technology, businesses of all sizes are expanding their technological capabilities and relying more and more on online transactions. Theft of intellectual property, manipulation of financial data, disruption of interactions with workers or business partners, manipulation of electronic ownership, harm to an organization's reputation, and eventual shutdown of e-commerce (or the whole firm) are all consequences of cybercrime.

Cybercriminals see the internet as a sweet treat because of the new way of doing business, which relies on electronic media. This includes banking, retail, and more. Businesses that are shifting their focus to the web are both thrilled about the opportunities for expansion and anxious about potential threats to customer data. Cybercrime threatens their whole data and financial system.

There are distinct difficulties and dangers associated with the e-commerce sector due to its distinct operations, such as the fact that fraud and crimes are more likely to occur in the absence of a physical presence. In India, there are a lot more factors that contribute to unregulated cyber fraud in the e-commerce sector. With more and more corporate operations shifting online and more and more people and groups from all over the globe congregating in cyberspace, the cost of cybercrime is only going to rise.

The parent firms lose a lot of money when their innovation rate drops because of the increased risk of intellectual property theft leading to copycat items made using stolen technology. If the government does not take decisive action to address cybercrime, businesses will be negatively impacted by technology. Annually, more than $400 billion is lost due to cybercrime throughout the world.

---

[3] Martellozzo E, *Cybercrime and Its Victims* 125-131 (Routledge, 2019).
[4] Sarika Digamber, "The study of frauds and safety in E-banking" 1(8) *AIJRRLSJM* 67-87 (2016).
[5] Mohammad Shahid Husain, *Critical concepts, standards, and techniques in cyber* forensics 121-125 (IGI Global, 2019).

There was a rise in criminal activity due to the physical collection of payments. The issue of incorrect delivery addresses, which results in significant financial losses for online retailers, is particularly common with COD alternatives. Data, information, and financial assets stored in cyberspace have been the subject of widespread concern due to various fraud incidents.[6]

3. THE RISE OF E-COMMERCE AND THE FIGHT AGAINST CYBERCRIME

3.1 The Rise of E-Commerce and Cybersecurity Challenges

When businesses and internet users work together, cybercrime may be reduced. Cybercrimes should be prevented with the help of organizations and governments that provide safety measures and technological assistance. People who use the internet also need to be careful not to become victims of electronic fraud. Combating such crimes is the shared obligation of users, governments, and e-commerce firms. Since software vulnerabilities are always being tracked, it is essential that computer programs be updated on a regular basis. In order to protect the computer systems from cybercriminals, it is important to have an antivirus program that can detect and eliminate malicious software.

"*Avnish Bajaj v. State (NCT of Delhi)*"[7] involved the CEO of Baazee.com, who was charged under the IT Act for hosting objectionable content sold via the platform. The Delhi High Court held that intermediaries are liable under certain conditions, emphasizing the responsibility of e-commerce platforms to monitor content and ensure compliance with cyber laws.

Online shopping has become the preferred method for most individuals these days. The fact that individuals would divulge sensitive information, including banking details, on these websites makes them a potential target for criminals.[8]

Therefore, in order to avoid falling for tempting offers from fraudulent websites, one should only buy on reputable websites, use different or similar passwords for each of the accounts; if hackers manage to breach one, they could be able to get them all. Passwords are more difficult to remember, but they offer an extra degree of security. Neither the debit nor the credit card numbers should be stored in the e-commerce websites.

"*Shreya Singhal v. Union of India*"[9] dealt with Section 66A of the Information Technology Act, 2000. The Supreme Court of India struck down the provision as unconstitutional, holding that it violated the right to freedom of speech and expression guaranteed under Article 19(1)(a) of the Constitution. While not directly about e-commerce, it highlighted the intersection of cyber laws and individual rights, paving the way for clearer regulatory frameworks in digital spaces.

Customers' personal information is vulnerable to hackers that breach the security chain of e-commerce websites' servers. For this reason, we should always take a little more time to input the card number. Scammers trick victims into divulging sensitive information (bank account numbers, social security numbers, etc.) by sending them fraudulent lottery or award-related emails.

Prior to their inclusion on the websites, merchants must undergo verification. It is important to verify that the consumer and the goods are authentic before processing their purchase. With this, the government has decided to combat cybercrime realizing that in order to lessen the impact of cybercrime, stringent rules and regulations should be strictly enforced.[10]

Although primarily about privacy, "*K.S. Puttaswamy v. Union of India*"[11] case indirectly impacted e-commerce by upholding the right to data privacy under Article 21 of the Constitution. It highlighted the obligation of e-commerce businesses to protect user data, influencing future cybersecurity policies.

3.2 Evolution and Impact of Cyber Regulations on E-Commerce and Data Privacy

Amidst widespread agreement that the cyber regulatory framework needed to be laid out, the Information Technology Act of 2000 was passed. In 1996, the United Nations Commission on International Trade law (UNCITRAL) published the model legislation on e-commerce in an effort to promote global consistency in cyber regulation.

Data privacy is discussed in further detail in the Information Technology Act; as the Internet continues to expand, more and more people's personal information is stored online, making it more susceptible to exploitation. An example of this kind of exploitation is the big data analysis. According to Big Data research, it is possible to influence people's decisions by studying their search patterns. In order to better identify and apprehend those responsible for cyber phishing, a new institution has been established by the new information technology legislation.

Cyber cafes were previously responsible for this type of attack, but now, following notification, customers are required to submit their personal ID to the store owner. This measure not only helps to trace the perpetrator but also serves as a deterrent. The Act has greatly enhanced the cyber investigation's resources by empowering an inspector to probe cyber offenses. The amendment expanded the authority to probe cyber offences from only the commissioner to include the inspector.

---

[6] Tejas Kashyap, "Impact of cyber-crimes on Indian economy" 4(2) *JSTOR* 116-123 (2017).
[7] 2005 (79) DRJ 576.
[8] Sameer Patil, *Securing India in the cyber era* 55 (Taylor & Francis Limited, 2021).
[9] AIR 2015 SC 1523.
[10] *Ibid.*
[11] AIR 2017 SC 4161.

As mentioned earlier, the UNCITRAL has recognized the e-commerce model legislation. However, as with any internationally recognized code, there are provisions meant to protect the sovereignty of individual states. As a result, local governments can still use the model laws as a guide, but they can still make their own decisions based on their own laws. Ever since the internet connected people on opposite sides of the world, end-user security has been a major worry. Now, hackers may more easily misuse victims' data or finances from the comfort of their own faraway locations.

Since the Internet is accessible from anywhere in the world, any court in the world may hear these cases. While it is true that cyber-contracts are legally binding and enforceable, determining which laws apply becomes a huge hurdle when the parties are located in different countries and haven't agreed on a particular provision.

The case "*Pawan Duggal v. State*"[12] involved online fraud wherein sensitive consumer data was compromised. The court emphasized the importance of implementing robust cybersecurity measures for businesses and held companies accountable for negligence in securing customer data, setting a precedent for data protection in e-commerce.

As there are so many vendors, buyers, and items involved in global e-commerce, it may be difficult to maintain restrictions on copyright violations. The internet, which can be accessed from anywhere in the world with very little preparation, is the environment where electronic commerce takes place. When it comes to time and distance, the traditional obstacles that businesses encounter do not apply to online marketplaces.[13]

Since the amount of time and energy put into anything is directly proportional to its value, it seems to reason that online shopping would be more cost-effective than traditional methods of doing business in near future.

4. CONCLUSION AND SUGGESTIONS

Although online shopping is distinct from traditional brick-and-mortar stores, it nonetheless has its own set of pros and cons. The Information Technology Act of 2000 was enacted with the intention of creating a cyber regulatory framework in line with the model laws established by UNCITRAL. The parties involved in an online transaction determine the kind of e-commerce that is engaged in and the worldwide nature of these e-commercial transactions raises a number of security, jurisdiction, taxes, etc. related issues. When dealing with the e-commerce system, it is important to understand the pros and cons of the system.

Integrity and morality are fundamental to any profession. The Company has an ethical and legal obligation to protect its customers' personal information by keeping it private and using encryption to prevent unauthorized access. Companies also have an ethical need to be honest about the quality of their goods and they shouldn't make false promises to customers in order to win their allegiance.

Suggestions-

- **Establishing Specialized Cybercrime Units:** Creating dedicated units with forensic tools and trained personnel to effectively investigate and combat sophisticated cybercrimes.
- **Enacting Data Protection Laws:** Implementing robust laws ensuring personal data security and privacy, aligned with global standards like GDPR.
- **Enhancing International Collaboration:** Strengthening global partnerships for intelligence sharing, cross-border investigations, and cybercriminal extradition.
- **Developing Victim Support Systems:** Offering legal aid, helplines, and psychological support for cybercrime victims.
- **Promoting Cyber Awareness Campaigns:** Educating citizens on cybersecurity practices to prevent phishing, fraud, and hacking.

REFERENCES

- Dueep J. Singh, *Introduction to Internet Scams and Fraud - Credit Card Theft, Work-At-Home Scams and Lottery Scams* 46-57 (Mendon Cottage Books, 2015).
- Rohan Nagpal, "Offences and penalties under the Information Technology Act, 2000" 8 *Information Technology Law Journal* 18-45 (2002).
- Martellozzo E, *Cybercrime and Its Victims* 125-131 (Routledge, 2019).
- Sarika Digamber, "The study of frauds and safety in E-banking" 1(8) *AIJRRLSJM* 67-87 (2016).
- Mohammad Shahid Husain, *Critical concepts, standards, and techniques in cyber* forensics 121-125 (IGI Global, 2019).
- Tejas Kashyap, "Impact of cyber-crimes on Indian economy" 4(2) *JSTOR* 116-123 (2017).
- Sameer Patil, *Securing India in the cyber era* 55 (Taylor & Francis Limited, 2021).

[12] 2001 CRILJ 3918.
[13] Information and Technology Act, 2000.