Effect of Cybercrimes on Working Women in Mumbai: The Financial and Psychological Implications

[1]Sejal Suresh Bothara, [2]Dr. Rupali Jitendra Khaire

[1]Ph.D Scholar, [2]Professor, School of Commerce and Management Studies , Sandip University , Nashik , Maharashtra , India

[1]sejalj5@gmail.com, [2]dr.rupalikhaire@gmail.com

Abstract

The growing reliance on the digital platforms and online financial transactions has led to the women employees being more susceptible to cybercrimes in metro cities such as Mumbai. This paper is provided both financial and non-financial consequences of cybercrimes on working women. Survey research conducted on 360 women employees in various sectors of Mumbai. A structured questionnaire was used to collect primary data and secondary sources like NCRB reports, RBI Ombudsman and Mumbai Police statistics were consulted. The findings indicate that over a third of the respondents had suffered financial cybercrimes, and the incidence was more in the banking, finance, IT, and retail industries. The most typical forms of crime proved to be phishing, UPI fraud, and e-commerce scam. The victims also experienced loss of money as well as stress, stigma, work disruption and loss of trust in the digital space. The paper comes to a conclusion that cybercrimes against working women are not purely financial problems but rather social and psychological problems as well that need to be addressed through awareness programmes and good redressal grievance mechanisms.

Introduction

Over the last few years, cybercrime has become one of the biggest challenges to online security in the world, and it impacts individuals, organizations, and countries. The emergence of the internet and the mobile technologies has created new opportunities of crime as cybercriminals take advantage of the anonymity and accessibility present in the digital world to commit crimes like fraud, identity theft, harassment, and hacking (Brown et al., 2009). Mumbai is one of the biggest and technologically advanced cities in India and working women in Mumbai have been especially vulnerable to financial and non-financial cybercrimes. Inadequate cybersecurity awareness, social inequalities, and greater digital interaction at work and in personal life are some of the factors that compound this weakness. The economics of cybercrime among working women in Mumbai are complex and can be classified as direct and indirect. The former can be the loss of money through online fraud or identity theft, the latter can include the time spent on resolving the identity theft and other problems (Lagazio et al., 2014). In addition to these material financial impacts, there are non-material impacts like emotional distress, reputation damage, and psychological damage that may be very detrimental to the well-being of the victims (Van Wilsem, 2013). The challenges that women in Mumbai have to deal with as they engage with the digital economy are unique to them, including the increased possibilities of online harassment, which only adds to risks that women have to face in the workplace (Yar, 2005; Kigerl, 2012). These implications are vital in establishing the measures to curb the effects of cybercrime on this group.

This study aims to explore both the financial and non-financial consequences of cybercrimes on working women in Mumbai, shedding light on how digital vulnerabilities uniquely affect them in the context of their professional lives. The findings would provide insights into the broader impact of cybercrime on gendered experiences of technology, while highlighting the need for tailored cybersecurity measures and policies to safeguard working women in urban India.

Direct financial burdens: extortion, identity theft, and productivity loss

Indian and comparative literature on cyber victimization indicates that women are generally targeted with financially driven victimization, such as sextortion, blackmail following image morphing, payment-fraud/credential theft, and expenses associated with infected devices and accounts. The corpus by Halder & Jaishankar on cybercrimes against women sets the tone of online harassment as it mixes with exploitation dynamics that may progress to financial coercion and reputation extortion as a form of payment, a trend that applies to urban, working women who have to maintain a digital profile in the public domain. In their initial studies of cyberstalking and harassment, Bocij and colleagues also predict practical fees (lost labor time, security expenses, legal consultation) incurred by the organization and victims of abuse that overflows into the workplace. Cumulatively, these strands hint that in a metropolis such as Mumbai, where the levels of digital transactions and social media presence are high, women professionals are subjected to both direct losses (extortion/ID theft) and diffuse economic burdens (downtime, remediation, and vigilance costs).

Psychological and social tolls that impair career trajectories

The non-financial effects reported throughout the bibliography anxiety, fear, shame, and withdrawal to social situations- overlap with well-researched harassment dynamics that inhibit performance and promotion. Articles covering cyberbullying, stalking, and gendered online abuse (e.g., Hinduja & Patchin; Spitzberg & Cupach; Halder & Jaishankar) explain stress reactions, presenteeism/absenteeism, and the suppression of civic participation (which can be particularly devastating to working women whose jobs involve networking, dealing with clients, or being visible in society). Theoretical frames (e.g., Nussbaum on shame and law) can be used to explain how reputational risks and moralized scrutiny compound emotional harms, and the modalities of online harassment also demonstrate how persistence and ubiquity can compound those harms even beyond office hours (e.g., technology-enabled stalking). Such non-financial expenses are career-related: loss of confidence, lost opportunities, and limited digital presence that are compounding factors of professional stagnation.

Legal and institutional context shaping redress in India (with Mumbai salience)

The bibliography points to India's dual framework—IPC and the IT Act-supplemented by evidence and procedural statutes, while comparative references (UK, Canada, US) illustrate broader policy toolkits against harassment and misuse of communications systems. This combination implies that the redress options available to the working women of Mumbai are dependent on provisions that are interpretable (e.g., criminal intimidation, defamation, obscenity, data misuse) and on effective policing capability. The mentioned acts and codes also presuppose compliance obligations on the part of platforms/employers (e.g., cooperation, retention of evidence), which have relevance to the speed at which victims will be able to reinstate accounts and mitigate reputational damage and losses. The loopholes highlighted in the wider literature, of jurisdiction, definitional scope, and enforcement, become transaction costs to victims (time, counsel, follow-up) that are, in practice, financial, even when the harms are not pecuniary.

Urban cyber-risk patterns and response capacity in Mumbai

Media and web items in the references document India-specific patterns—morphed images, social-media blackmail, and credential compromise—while the Mumbai Police Cyber Cell case-study link underscores local enforcement and incident typologies, including financially oriented intrusions. For working women in Mumbai's service and knowledge sectors, these patterns matter: mobile-first usage, dense professional networking online, and high digital payment adoption can raise exposure to targeted phishing, account takeovers, and reputational attacks that prompt costly containment measures (forensic checks, legal notices, PR repairs). The literature's emphasis on awareness/advocacy resources further indicates that outcomes improve where victims and employers act swiftly—collecting evidence, engaging platforms, and coordinating with cyber cells—mitigating both monetary loss and cascading psychosocial harm.

METHODOLOGY

This research adopts a mixed-methods design, integrating both primary and secondary data sources in order to examine the financial and non-financial implications of cybercrimes on working women in Mumbai. The combination of direct data collection through surveys and interviews, together with official records and reports, ensures both empirical depth and contextual accuracy.

Primary Data

The primary data consist of a structured survey administered to 360 working women in Mumbai, selected through stratified random sampling to ensure proportional representation across six occupational sectors: information technology, banking and finance, education, healthcare, retail and e-commerce, and small business or entrepreneurship. The questionnaire collected demographic information (age, income, education, and sector of employment), experiences of financial cybercrimes such as phishing, UPI fraud, card cloning, identity theft, and e-commerce scams, as well as non-financial impacts including stress, stigma, workplace disruption, and loss of trust in digital platforms. It also included questions on awareness and reporting behavior in relation to the National Cyber Crime Reporting Portal, the Mumbai Cyber Cell, and RBI grievance systems.

In addition, semi-structured interviews were conducted with 20–25 working women who reported experiences of cybercrime. These interviews explored the psychological and social consequences of victimization, barriers to reporting, and coping strategies. Further interviews with cybercrime investigators, NGO representatives, and HR professionals were conducted to capture institutional perspectives.

Secondary Data

The secondary data were obtained from official and published sources that provide statistical and contextual background on cybercrime. The study analyzed National Crime Records Bureau (NCRB) reports (2020–2023) for state and national cybercrime trends, Mumbai Police Cyber Cell records for city-level case reports of financial fraud and online harassment, and Reserve Bank of India Ombudsman reports (2020–2024) for banking-related fraud complaints. Additional insights were drawn from existing scholarly research, government publications, and credible media reports that illustrate the prevalence and patterns of cybercrime in urban contexts. These secondary data were used to validate and compare with the findings from the primary data, strengthening the reliability of the study through triangulation.

Analysis

The survey data were analyzed using descriptive and inferential statistics, including frequency distributions, cross-tabulations, chi-square tests, and logistic regression to identify predictors of victimization and reporting. Interview transcripts were examined using thematic analysis (Braun & Clarke, 2006) to identify recurring themes such as fear, stigma, trust deficits, and workplace responses. Secondary data were systematically reviewed and compared with primary findings to highlight consistencies, contradictions, and gaps. In addition, a legal analysis was conducted by reviewing relevant provisions of the Information Technology Act (2000, amended 2008), the Indian Penal Code, and regulatory guidelines issued by the Reserve Bank of India.

RESULT AND DISCUSSION

The study surveyed 360 working women in Mumbai across six sectors (Table 1B). The largest group was from Information Technology (20%), followed by Banking & Finance (18.1%), and Education (16.9%). Respondents' average age was 36.0 years (SD = 8.25), ranging from 22 to 50 years (Table 1A). Educational qualifications were balanced between undergraduates (43.3%) and postgraduates (41.1%), with 15.6% holding professional certifications (Table 1C). In terms of monthly income, the majority earned between ₹25,000–₹1,00,000 (63.6%), while 21.4% earned above ₹1,00,000 (Table 1D).

Table 1A. Sample Profile (Age Summary)

N_total	Age_mean	Age_sd	Age_min	Age_p25	Age_p50	Age_p75	Age_max
360.0	36.04	8.25	22.0	29.75	35.0	42.25	50.0

Table 1B. Sample Profile by Employment Sector

Employment_sector	N	%
Information Technology	72	20.0
Banking & Finance	65	18.1
Education	61	16.9

Healthcare	54	15.0
Retail & E-commerce	54	15.0
Small Business/Entrepreneurship	54	15.0

Table 1C. Education Distribution

Education	n	%
Undergraduate	156	43.3
Postgraduate	148	41.1
Professional/Certification	56	15.6

Table 1D. Monthly Income Band Distribution

Monthly_income_band	N	%
₹50k–₹1L	116	32.2
₹25k–₹50k	113	31.4
₹1L–₹2L	60	16.7
< ₹25k	54	15.0
> ₹2L	17	4.7

Prevalence of Financial Cybercrime

Overall, 36.4% of respondents (n=131) reported experiencing at least one financial cybercrime (Table 2A). Victimization rates varied across sectors: highest in Banking & Finance (50.8%), followed by Retail & E-commerce (46.3%) and Information Technology (37.5%). Lower rates were observed in Education (32.8%), Healthcare (27.8%), and Small Business/Entrepreneurship (20.4%) (Table 2B).

Table 2A. Overall Victimization

Measure	N	% of sample
Victimization (experienced_financial_cybercrime = 1)	131	36.4

Table 2B. Victimization by Employment Sector

Employment_sector	N_in_sector	Victimization_rate_%
Banking & Finance	65	50.8
Education	61	32.8

Healthcare	54	27.8
Information Technology	72	37.5
Retail & E-commerce	54	46.3
Small Business/Entrepreneurship	54	20.4

Types of Financial Cybercrime

The most common forms of financial cybercrime were UPI fraud (15.8% of all respondents; 43.5% of victims), phishing (13.6%; 37.4%), and e-commerce scams (12.5%; 34.4%) (Table 2C). Card cloning (6.9%; 19.1%) and identity theft (6.7%; 18.3%) were less prevalent but still significant.

Table 2C. Distribution of Financial Cybercrime Types

Financial cybercrime type	Percent of all respondents (%)	Percent of victims (%)
phishing	13.6	37.4
upi_fraud	15.8	43.5
card_cloning	6.9	19.1
identity_theft	6.7	18.3
ecommerce_scam	12.5	34.4

Awareness and Reporting

Awareness of grievance mechanisms was moderate: Mumbai Cyber Cell (57.5%) had the highest awareness, followed by the National Portal (53.3%) and RBI Ombudsman (47.8%) (Table 3A). However, reporting was limited: nearly four in five victims (79.4%) did not report incidents. Among the few who did report, 11.5% approached the Mumbai Cyber Cell, 6.1% the National Portal, and 3.1% the RBI Ombudsman (Table 3B & 3C).

Table 3A. Awareness Rates

Awareness channel	Awareness rate (%)
National Portal	53.3
Mumbai Cyber Cell	57.5
RBI Ombudsman	47.8

Table 3B. Reporting Channels among Victims

Reporting channel	n	% of victims
None	104	79.4
Mumbai Cyber Cell	15	11.5

National Portal	8	6.1
RBI Ombudsman	4	3.1

Table 3C. Reporting vs Non-reporting among Victims

Measure	% of victims
Reported any channel	20.6
Did not report	79.4

Non-Financial Impacts

Cybercrime victims reported significantly higher non-financial impacts than non-victims (Table 4). Stress levels averaged 2.37 vs. 1.27, stigma 1.44 vs. 0.85, work disruption 1.61 vs. 0.86, and trust loss 1.9 vs. 1.14 (on a 0–4 scale). Victims also reported an average time loss of 26 hours, compared to negligible time loss among non-victims.

Table 4. Non-financial Impacts by Victimization Status

Experienced_financial_cybercrime	Stress_level_0to4	Stigma_level_0to4	Work_disruption_0to4	Trust_loss_0to4	Time_lost_hours
No	1.27	0.85	0.86	1.14	0.0
Yes	2.37	1.44	1.61	1.9	26.0

Discussion

The paper identifies the multidimensionality of cybercrimes as a burden to working women in Mumbai. The prevalence is high with more than a third of respondents being victimized, and there is sectoral variation that highlights an occupational risk.

Sectoral Exposure

Banking, finance and retail/e-commerce, which rely heavily on online transactions and UPI payments, had the highest victimization rates. These data are reflected in Reserve Bank of India Ombudsman reports which regularly cite unauthorized electronic transactions as a category of complaints in the top-ranking bracket. The smaller rates in healthcare and small businesses could indicate the decreasing exposure to digital payments in everyday work.

Nature of Cybercrime

The dominance of UPI fraud and phishing illustrates how cybercriminals exploit India's rapid shift to digital payments. Similar to global studies, scams relying on social engineering are the most common. While identity theft and card cloning are less frequent, they still represent nearly one in five victim experiences, signaling persistent risks beyond newer payment systems.

Awareness–Reporting Gap

A critical finding is the disconnect between awareness and reporting. Despite half of the respondents knowing about official grievance mechanisms, only 20.6% of victims reported incidents. This suggests systemic barriers: lack of trust in institutional redress, perceived complexity of reporting, and fear of stigma. The Mumbai Police's own reports acknowledge severe under-reporting in cybercrime cases, which this survey confirms.

Non-Financial Consequences

The study shows that financial loss is only one dimension of harm. Victims experienced elevated stress, workplace disruption, stigma, and loss of trust in digital platforms. These findings echo Halder & Jaishankar (2017), who argue that women face unique psychosocial burdens in cybercrime victimization, and Powell & Henry (2018), who link digital victimization with erosion of digital confidence. For working women, the reported 26 hours of lost time translates into productivity decline, underscoring that cybercrime has both economic and occupational implications.

Policy and Organizational Implications

The findings highlight the need for multi-level interventions. At the policy level, simplifying reporting processes, ensuring confidentiality, and enhancing victim support in Mumbai Cyber Cell can address under-reporting. At the organizational level, employers — especially in finance, IT, and retail — should integrate cyber hygiene training into workplace culture and provide supportive HR policies for victims. Gender-sensitive grievance mechanisms, rapid dispute resolution by RBI Ombudsman schemes, and targeted awareness campaigns could collectively reduce both financial and non-financial impacts.

Limitations and Future Work

The study relies on self-reported data, which may involve recall bias or underreporting due to stigma. While the sample is sectorally diverse, it is restricted to Mumbai, limiting generalizability. Future research should include comparative studies across Indian metros, triangulation with police and bank records, and longitudinal tracking of victim recovery outcomes.

Conclusion

The study clearly shows that cybercrimes have a significant impact on working women in Mumbai. Over one-third of the surveyed people have been the victims of cybercrimes with those in the banking, finance, IT, and retail industries being more vulnerable to cybercrimes as they are more exposed to online platforms. Although financial losses were different in cases, non-financial outcomes like stress, stigma and work disruption were found to be equally severe outcomes. This was despite the moderate level of awareness regarding reporting mechanisms, most victims were not reporting incidents, which indicates systemic obstacles and the failure to trust redressal. To overcome these issues, gender-sensitive cybercrime help systems, easy reporting system, and workplace-based awareness campaigns are required. It is important to enhance cyber cells, enhance the coordination of financial institutions, and enhance the culture of digital safety to minimize the occurrence and the effect of cybercrimes on working women.

REFERENCES

Journals

1. Brown, I., Edwards, L., & Marsden, C. (2009). *Information security and cybercrime, law and the internet* (3rd ed.). L. Edwards & C. Waelde (Eds.). Oxford University Press.

2. Kigerl, A. (2012). Routine activity theory and the determinants of high cybercrime countries. *Social Science Computer Review, 30*(4), 470-486. https://doi.org/10.1177/0894439312458481

3. Lagazio, M., Sherif, N., & Cushman, M. (2014). A multi-level approach to understanding the impact of cybercrime on the financial sector. *Computers & Security, 45*, 58-74. https://doi.org/10.1016/j.cose.2014.03.005

4. Saini, H., Rao, Y.S., & Panda, T.C. (2012). Cyber-crimes and their impacts: A review. *International Journal of Engineering Research and Applications (IJERA), 2*(2), 202-209.

5. Van Wilsem, J. (2013). Hacking and harassment—Do they have something in common? Comparing risk factors for online victimization. *Journal of Contemporary Criminal Justice, 29*(4), 437-453. https://doi.org/10.1177/1043986213495162

6. Yar, M. (2005). The novelty of 'cybercrime': An assessment in light of routine activity theory. *European Journal of Criminology, 2*(4), 407-427. https://doi.org/10.1177/1477370805057845

7. Halder, D., & Jaishankar, K. (2008). Cyber crimes against women in India: Problems, perspectives and solutions. *TMC Academic Journal, 3*(1), 48–62.

8. Hinduja, S., & Patchin, J. W. (2011). Cyberbullying: Identification, prevention, and response. *Cyberbullying Research Center*. Retrieved from https://cyberbullying.us

9. Spitzberg, B. H., & Cupach, W. R. (2007). The state of the art of stalking: Taking stock of the emerging literature. *Aggression and Violent Behavior, 12*(1), 64–86. https://doi.org/10.1016/j.avb.2006.05.001

10. Government of India. (2000). *The Information Technology Act, 2000 (as amended in 2008).* Ministry of Law, Justice and Company Affairs. Retrieved from https://www.meity.gov.in/

11. Government of India. (1860). *The Indian Penal Code, 1860 (as amended).* Ministry of Law and Justice. Retrieved from https://legislative.gov.in/

12. Mumbai Police. (2023). *Annual report of the Cyber Crime Cell, Mumbai.* Mumbai Police Headquarters. Retrieved from https://mumbaipolice.gov.in/

13. National Crime Records Bureau (NCRB). (2021). *Crime in India 2020: Statistics.* Ministry of Home Affairs, Government of India. Retrieved from https://ncrb.gov.in/

14. National Crime Records Bureau (NCRB). (2022). *Crime in India 2021: Statistics.* Ministry of Home Affairs, Government of India. Retrieved from https://ncrb.gov.in/

15. National Crime Records Bureau (NCRB). (2023). *Crime in India 2022: Statistics.* Ministry of Home Affairs, Government of India. Retrieved from https://ncrb.gov.in/

16. Reserve Bank of India (RBI). (2021). *Annual report of the Ombudsman Schemes 2020–21.* Reserve Bank of India. Retrieved from https://rbi.org.in/

17. Reserve Bank of India (RBI). (2022). *Annual report of the Ombudsman Schemes 2021–22.* Reserve Bank of India. Retrieved from https://rbi.org.in/

18. Reserve Bank of India (RBI). (2023). *Annual report of the Ombudsman Schemes 2022–23.* Reserve Bank of India. Retrieved from https://rbi.org.in/

19. Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology, 3*(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

20. Halder, D., & Jaishankar, K. (2017). *Cyber crimes against women in India.* SAGE Publications.

21. Powell, A., & Henry, N. (2018). *Sexual violence in a digital age.* Palgrave Macmillan.

Books

- Bocij, P. (2004). *Cyberstalking: Harassment in the Internet age and how to protect your family*. Westport, CT: Praeger.

- Halder, D., & Jaishankar, K. (2012). *Cyber crime and victimization of women: Laws, rights, and regulations*. Hershey, PA: IGI Global.

- Halder, D., & Jaishankar, K. (2017). *Cyber crimes against women in India*. London: Sage.

- Nussbaum, M. C. (2004). *Hiding from humanity: Disgust, shame, and the law*. Princeton, NJ: Princeton University Press.