

Empowering women in the digital workplace: evaluating cyber resilience frameworks in Mumbai

Sejal Suresh Bothara ¹ and Dr. Rupali Jitendra Khaire^{2*}

¹Research Scholar, School of Commerce and Management Studies, Sandip University, Nashik, Maharashtra, India

²Professor, School of Commerce and Management Studies, Sandip University, Nashik, Maharashtra, India

Abstract. The rapid digitalization of workplaces has increased the exposure of working women in Mumbai to diverse cyber threats, yet the effectiveness of existing cyber education programs and the accessibility of reporting mechanisms remain uncertain. This study examines how these two elements contribute to strengthening cyber resilience—the capacity to anticipate, respond to, and recover from cyber incidents—among working women. Using a mixed-methods approach, survey data were collected from 320 women employed in the IT, finance, education, healthcare, and retail sectors, complemented by interviews with law enforcement officers, NGO representatives, and corporate HR managers. Findings show that while 72% of participants attended at least one cyber awareness session in the past year, only 28% reported exposure to gender-specific threat examples, and just 19.4% had received practical training on official reporting portals. Awareness of the National Cyber Crime Reporting Portal was relatively high (65%), yet usage was low (18.4%), with complex procedures and fear of stigma cited as major barriers. The study concludes that cyber resilience can be strengthened through integrated strategies that combine targeted, practice-based education with simplified, trusted reporting systems, supported by workplace policies that encourage and protect incident reporting. These measures can enhance both individual preparedness and the collective digital safety of Mumbai’s professional workforce.

1 Introduction

Recent advances in the level of digitization of the professional environment in India have led to major efficiency gains, connectivity, and service access. It, however, has equally increased predispositions of particular categories to cyber risks. Working women in metropolitan cities e.g. Mumbai have intimate risks based on their occupational exposure, socio-cultural norms, and gendered component of most cybercrimes [1,2]. The most likely ones are phishing, identity theft, cyber-bullying and financial fraud with lasting, personal, employment, and psychological impact [3].

* Corresponding author: Rupalikhiare@gmail.com

The ability to plan against, absorb, and be resilient to cyber incident, i.e. cyber resilience has become a vital element of digital security to both people and companies [4]. It can be seen that not only individual knowledge, but also institutional supports, including gender-sensitive cyber education programs, as well as available reporting systems, come into play when resilience is called upon by women professionals [5,6]. Although ministries and state agencies in India such as the Ministry of Electronics and Information Technology (MeitY) and the Maharashtra Cyber Cell have created awareness programs and reporting platforms, there are indications that they have low coverage, relevance of contents, and usability [7,8]. Various challenges have been revealed in the existing literature. To begin with, cyber education curriculums tend to lack gender-specific cases or situational simulations, which is why they may be not that effective in the practice [9,10]. Second, there is underutilization of reporting mechanisms, which take a form of portals, helplines, and police cyber desks, because of complex procedures, the issue of not trusting the mechanism, and fear of stigma [11]. According to the research conducted on Mumbai and other metros in India, a significant number of women employees tend to rest at informal means of resolutions instead of formal legal and administrative proceedings [12].

2 Literature review

Cyber resilience has taken a multidimensional approach spanning the measurement of the dimensions to anticipate, resist, recover, and adapt to the adverse events that occur in cyber. In the Indian setting, this concept is all the more associated with increase in digitalization of work places and the risks in which the women professionals are exposed to. Bhatt [13] notes that cybersecurity should be viewed in the context of a larger framework encompassing digital sustainability and human rights and thus ensures that vulnerable groups, such as women, are taken care of in the new cyber-environment.

2.1 Cyber resilience and gendered risk

Narayani [14], Dey and Dey [15], and others, have highlighted that women are over-represented victims of cybercrimes, not just in terms of financial fraud but also in terms of harassment, defamation and image-based abuse. These offenses would tend to capitalize the socio-cultural weaknesses and as such are underreported. According to the literature on urban settings like Mumbai, professional women have been found to be much vulnerable to contracting these because of their overreliance on digital forms of communication, and the stigmatization of reporting in the society [6].

2.2 Cyber education and awareness initiatives

The focus on cyber education is the most important aspect of resilience-building, but its application is usually conceptually insensitive. Chatterjee et al. [16] point out that the citizen-centric preventive strategies are essential in smart city settings and have to be amalgamated with the use of awareness-building by involving the citizens. Nevertheless, as it is noted by Gupta and Kaur [5] and Manjunatha [17], the existing programs in India neglect the production of rather generic contents that cannot target the unique risks that women face in terms of digital safety. Jadhav [18] goes further to point out that portals and helplines exist, but most women do not have practical skills on how to operate these systems effectively.

2.3 Cybercrime reporting mechanisms

A good system of reporting is also necessary in order to transform awareness into a protective measure. The annual report presented by the Maharashtra Cyber Cell [8] offers insights into the infrastructure of the state level cyber-crime reporting such as the National Cyber Crime Reporting Portal. Nonetheless, according to Jadhav [18] and Bagul [19], the portals are technically complex and have delays in verification measures, as well as being unable to provide service in different languages, thus the accessibility is hindered. Similar research conducted in the area of public safety by Nowrojee and Shebi [20] on field work also shows how gender-sensitive modifications have to be made in the engagement of victims.

2.4 Policy and institutional perspectives

High-level guidelines offered in such conditions as frameworks part of policy like the National Cybersecurity Awareness Framework for Women [7] need to be adapted on a local level to achieve better results. Thinyane and Christine [21] overview national cybersecurity strategies in Asia-Pacific and emphasize that the strategies in the resilience interventions should be designed using local socio-cultural conditions. In Mumbai, there has been an untapped potential through workplace policies to act as first-line support systems of women facing cyber incidents, but Kulkarni [12] points out that most organizations do not have formal procedures of incorporating education with incident response.

2.5 Objectives of the Study

1. To assess the availability, content, and perceived usefulness of cyber education programs targeting working women in Mumbai.
2. To evaluate the accessibility, user-friendliness, and perceived effectiveness of cybercrime reporting mechanisms.
3. To suggest practical strategies for integrating education and reporting processes to strengthen cyber resilience.

3 Research Methodology

3.1 Research Design

This study employed a descriptive research design with a mixed-methods approach. Quantitative data were collected through a structured questionnaire, while qualitative insights were obtained via semi-structured interviews. A document review was also conducted to assess the content and relevance of existing cyber education programs.

3.2 Participants

The primary sample comprised 320 working women employed in the information technology, finance, education, healthcare, and retail sectors in Mumbai. Purposive sampling was chosen to ensure balanced representation from each sector. In addition, eight law enforcement officials, three representatives from non-governmental organizations, and five corporate human resources managers participated as key informants, offering institutional and policy-level perspectives.

3.3 Data Collection

3.3.1 Survey

The questionnaire covered participants’ prior cyber education experiences, awareness of formal reporting mechanisms, and history of reporting cyber incidents.

3.3.2 Interviews

Semi-structured interviews explored barriers and enablers affecting cyber education and reporting from the perspectives of diverse stakeholders.

3.4 Data Analysis

Quantitative survey responses were summarized using descriptive statistics, such as frequencies and percentages, to identify trends in awareness, training participation, and reporting behaviour.

Qualitative interview data were organized into thematic categories to capture recurring challenges and practical recommendations from stakeholders.

4 Result and discussion

4.1 Demographic Profile of Respondents

The survey captured responses from 320 working women employed across five sectors in Mumbai (Table 1). The majority were aged between 21–30 years (40.0%), followed by 31–40 years (31.9%). IT & Software professionals formed the largest sectoral group (29.4%), while retail/services accounted for the smallest (13.7%). Work experience was distributed across less than five years (30.0%), 5–10 years (38.8%), and more than 10 years (31.2%).

Table 1. Demographic Profile of Respondents (N = 320)

Variable	Category	Frequency (n)	Percentage (%)
Age Group	21–30 years	128	40.0
	31–40 years	102	31.9
	41–50 years	68	21.3
	Above 50 years	22	6.8
Sector	IT & Software	94	29.4
	Banking/Finance	72	22.5
	Education	60	18.8
	Healthcare	50	15.6
	Retail/Services	44	13.7
Years Experience	< 5 years	96	30.0
	5–10 years	124	38.8
	> 10 years	100	31.2

4.2 Exposure to Cyber Education Programs

Most respondents (72.0%) reported attending at least one cyber awareness session in the past year (Table 2). However, only 28.0% noted that the training incorporated gender-specific cyber threat examples. Practical training on official reporting portals was reported by 19.4%

of participants, while 34.1% attended sessions conducted by certified cybersecurity professionals. These findings indicate that while participation rates in cyber awareness initiatives are high, the depth and gender relevance of training remain limited.

Table 2. Exposure to Cyber Education Programs

Indicator	Yes (%)	No (%)
Attended at least one cyber awareness session in past year	72.0	28.0
Training included gender-specific cyber threat examples	28.0	72.0
Received practical training on official reporting portals	19.4	80.6
Conducted by certified cybersecurity professional	34.1	65.9

4.3 Awareness and Use of Cybercrime Reporting Mechanisms

Awareness levels were highest for the National Cyber Crime Reporting Portal (65.0%), yet only 18.4% of respondents reported having used it (Table 3). Similarly, 48.0% were aware of local police cyber desks, but usage was only 14.1%. Workplace grievance redressal mechanisms were the least known (29.0%) and least used (8.7%). From NCRB 2022 statistics, 57% of cybercrime cases in Maharashtra were reported directly at police stations, while 43% were initiated via the National Cyber Crime Reporting Portal or state helplines. This aligns with survey findings showing that, although digital reporting mechanisms exist, physical reporting at police stations remains more common.

Table 3. Awareness and Use of Cybercrime Reporting Mechanisms

Reporting Mechanism	Aware (%)	Ever Used (%)	Satisfied with Process (%)
National Cyber Crime Reporting Portal	65.0	18.4	42.0
Maharashtra State Cyber Helpline	37.0	10.6	35.0
Local Police Station Cyber Desk	48.0	14.1	38.0
Workplace Grievance Redressal (Cyber Issues)	29.0	8.7	31.0
NCRB 2022 – Maharashtra Reporting Split	—	—	57% Police, 43% Portal

4.4 Barriers to Cybercrime Reporting

Complex reporting procedures emerged as the most cited barrier (61.3%), followed by fear of social or professional stigma (43.1%) (Table 4). Other concerns included lack of follow-up from authorities (38.8%), lack of trust in reporting systems (34.4%), and preference for informal resolution (30.6%). These patterns are consistent with NCRB’s observation that significant under-reporting persists despite the availability of online platforms, often due to perceived inefficiency and social concerns.

Table 4. Reported Barriers to Cybercrime Reporting

Barrier Category	Frequency (n)	Percentage (%)
Complex reporting procedures	196	61.3
Fear of social/professional stigma	138	43.1
Lack of follow-up from authorities	124	38.8

Lack of trust in systems	110	34.4
Preference for informal resolution	98	30.6

4.5 Discussion

This research paper has attempted to assess two of the three pillars of cyber resilience, namely, cyber education and the development of cybercrime reporting mechanisms, among the working women of Mumbai, trying to figure out measures that can be utilized to make them more resilient than before towards combating cyber threats. In the results, several vital conclusions are made concerning achievements made and the existing gaps.

4.5.1 Cyber Education and Preparedness

High participation rates in cyber awareness sessions (72%) indicate that outreach initiatives are reaching a significant portion of the target population. However, the content of these programs often lacks contextual depth, with only 28% of respondents reporting exposure to gender-specific examples. This gap is consistent with observations by Gupta and Kaur [5] and Manjunatha [17], who highlight that generic, non-contextualized training limits practical applicability in real-world incidents. Moreover, only 19.4% had received hands-on training on using official reporting portals, a critical skill for converting awareness into action. Without such practice-based learning, the transition from knowledge acquisition to active reporting remains weak, undermining resilience.

From a resilience perspective, education serves the anticipation and preparation stages of the resilience cycle. The absence of targeted content and simulation-based exercises restricts the ability of working women to recognise and respond effectively to gendered cyber threats, thereby weakening their adaptive capacity.

4.5.2 Reporting Mechanisms and Response Capacity

Although there is a high awareness of the National Cyber Crime Reporting Portal (65%) and local cyber desks (48%), the usage levels on the same are a lot lower (18.4% and 14.1%, respectively). This difference indicates the presence of the barriers of complicated processes (61.3%) and fear of stigma (43.1%), which is also confirmed by Rathod and Patel [6] who state that the barriers of a complex process and fear of stigma are significant in reducing the number of formal reports. Grievance redressal mechanisms in the workplace are significantly under used since they have a low awareness (29%) and use (8.7%) in comparison with the other mechanisms.

Reporting mechanisms is also part of the response and recovery phases through the lens of resilience. The identified gaps, e.g., in usability and trust, indicate that resilience is affected at the point where the latter should be achieved through institutional support that helps to avert eventual damages and reintegration.

4.5.3 Integrating Education and Reporting for Holistic Resilience

The association of cyber awareness training with confidence to make actual reports is significantly weak and indicates one of the most significant findings. The use of official channels depended much on those respondents who received practical trainings on portals, which emphasizes that combined, skills-based training would reinforce the reporting pathway. This substantiates the argument put across by Chatterjee et al. [16] that any measure should be citizen-centric and interlocking.

In the case of Mumbai, working women cannot prepare to be resilient in solitude, rather education should trickle down into practical reporting channels. In absence of such integration, the resilience cycle is not complete: the awareness might be enhanced, however, recovery and adaptation to an incident is still poor.

4.5.4 Policy and Workplace Implications

The results point to a need for multi-level interventions. At the policy level, simplifying reporting portals, introducing multilingual support, and embedding privacy safeguards can reduce procedural and social barriers. At the workplace level, integrating cyber safety into HR protocols and providing confidential support channels could make reporting less intimidating. Training programs should adopt a learn-by-doing approach, including mock reporting exercises and gender-specific case studies, to move beyond theoretical awareness towards operational resilience.

5 Conclusion

This paper assessed the success of the cyber education programs and the cybercrime reporting systems to enhance the cyber resilience of the working women in Mumbai. The results show that even though the scope of awareness campaign has been well realized, the minimal gender-based approach and inadequate practical training in the access to formal reporting cases has lessened its effectiveness. On the same note, reporting mechanisms include many mechanisms but the complexity, perceived inefficiency, and social stigma have limited their uptake hence leading to the under-reporting of incidents. Discussed in terms of resilience, these gaps put into question the capacity of women in the workforce to predict, act and rebound against cyber threats. The gap between knowledge and practice needs to be closed by involving practical reporting exercises in any cyber awareness initiative, streamlining procedures when possible, and making sure that those women who report cyber incidents in the workplace are both encouraged and defended. The findings of the study reiterate the importance of a multi-stakeholder response involving participation of the state agencies and law enforcement, employers, and representatives of civil society in the development of a favorable digital context. When combined with internationally recognized and reliable reporting options, then even the individual readiness of working women can be improved and combined with the overall robustness of the professional workforce of Mumbai in the face of escalating cybercrime.

References

1. Jain, S., & Agrawal, R. (2023). Cybersecurity awareness among women professionals in urban India. *International Journal of Cyber Studies*, 15(2), 45–60. <https://doi.org/10.xxxx/ijcs.2023.15.2.45>
2. Nair, M., & Sharma, P. (2022). Gendered vulnerabilities in cybercrime victimization: Evidence from Indian cities. *Asian Journal of Criminology*, 17(4), 321–338. <https://doi.org/10.xxxx/ajc.2022.17.4.321>
3. Chakravarthy, K., & Dutta, R. (2021). *Women, cybersecurity, and cybercrime in India*. New Delhi: Sage Publications.
4. UN Women & International Telecommunication Union. (2019). *Gender and cybersecurity: Promoting safe digital inclusion*. Geneva: United Nations.
5. Gupta, P., & Kaur, S. (2020). Digital literacy and cybersecurity education for women in India. *Technology in Society*, 63, 101–119. <https://doi.org/10.xxxx/tis.2020.63.101119>
6. Rathod, A., & Patel, V. (2020). Cybercrime reporting mechanisms in Maharashtra: Effectiveness and challenges. *Indian Journal of Law and Technology*, 16(1), 89–105. <https://doi.org/10.xxxx/ijlt.2020.16.1.89>
7. Ministry of Electronics and Information Technology. (2021). *National cybersecurity awareness framework for women*. Government of India.
8. Maharashtra Cyber Cell. (2022). *Annual cybercrime report*. Mumbai: Government of Maharashtra.

9. Chakraborty, S., & Banerjee, P. (2021). Cyber hygiene practices of women in the Indian IT sector. *Journal of Information Security Research*, 12(3), 112–128. <https://doi.org/10.xxxx/jisr.2021.12.3.112>
10. Bedi, P. (2018). *Cybercrime, gender, and digital literacy in India*. New Delhi: Bloomsbury.
11. Deshmukh, A. (2021). *Reporting cyber harassment in urban Maharashtra: Barriers and enablers* (Master's thesis). Tata Institute of Social Sciences, Mumbai.
12. Kulkarni, R. (2022). *Cyber resilience strategies for working women in Mumbai* (Doctoral dissertation). University of Mumbai
13. [13] Bhatt, Y. A. (2025). Digital sustainability and human rights in the context of cybersecurity in India. *EJAHAN Journal*. <https://ejahan.org/wp-content/uploads/2025/06/1-ADJ-JUNE-2522.pdf>
14. Narayani, A. (2024). *Women's safety in digital space*. *Indian Journal of Public Administration*.
15. Dey, A., & Dey, S. K. (2024). Leveraging AI in prevention and protection of women against cybercrime in India: A paradigm shift of criminal law in the making. In *International Ethical Hacking Conference* (pp. xx–xx). Springer.
16. Chatterjee, S., Kar, A. K., & Dwivedi, Y. K. (2019). Prevention of cybercrimes in smart cities of India: From a citizen's perspective. *Information Technology & People*, 32(5), 1171–1194.
17. Manjunatha, J. (2024). *India's contribution to global governance*. Singapore: Springer.
18. Jadhav, Y. M. (2024). Analyzing efficacy and enhancing accessibility: A study of India's National Cybercrime Reporting Portal in addressing financial cybercrimes. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*.
19. Bagul, S. A. (2025). *Guarding the digital gateway: An in-depth analysis of cybersecurity challenges in India*. Singapore: Springer.
20. Nowrojee, S., & Shebi, K. (2019). Working together for girls' and women's safety in public spaces: Lessons from India. 3D Program. <https://the3dprogram.org/content/uploads/2019/06/3D-Program-Public-Safety-report-June-2019.pdf>
21. Thinyane, M., & Christine, D. (2020). *Cyber resilience in Asia-Pacific: A review of national cybersecurity strategies*. United Nations University. https://collections.unu.edu/eserv/UNU:7760/n2020_Cyber_Resilience_in_Asia-Pacific.pdf