International Journal of Education, Modern Management, Applied Science & Social Science (IJEMMASSS)
An International Quarterly bi-lingual Multidisciplinary Double Blind Open Access Peer Reviewed Refereed Journal
ISSN:2581-9925, Impact Factor (Cosmos: 7.555 & I2OR: 5.105), Volume 08, No. 03(IV)(Special Issue), July-September, 2026, pp. 01-06

Impact of Digital Forensics Maturity on Cyber Resilience and Safety among Women Entrepreneurs

Alok Kumar Pandey[1*] | Dr. Ranjan Kumar Mishra[2]

[1,2]Netaji Shubas University, Jamshedpur, India.

[*]Corresponding Author: alok2pandey@gmail.com

DOI: Pandey, A., & Mishra, R. (2026). Impact of Digital Forensics Maturity on Cyber Resilience and Safety among Women Entrepreneurs. International Journal of Education, Modern Management, Applied Science &Amp; Social Science, 08(03(IV)), 1–6. https://doi.org/10.62823/ijemmasss/8.3(iv).9575

ABSTRACT

Business activities have become highly digitized, exposing female entrepreneurs in developing nations such as India to various cybersecurity challenges, including phishing attacks, data breaches, online scams, identity theft, and sexual cyberbullying. These security challenges not only threaten their livelihoods but also hinder their ability to use digital technology for conducting business and other commercial transactions. This research paper will explore the effect of digital forensics maturity on cyber resilience and safety among women entrepreneurs. Digital forensics maturity is defined by an organization or individual's ability to prepare for, analyse, and recover from attacks on information systems using sound methods, appropriate tools, and capable professionals, and by incorporating these practices into incident response processes. Maturity scales, such as those used to extend the Digital Forensics Readiness Commonalities Framework (DFRCF), evaluate maturity on a scale from a reactive process to one that is optimized and proactive. Greater maturity will result in more rapid attribution, evidence collection, reduced downtime, and improved defences. The findings will demonstrate that high digital forensics maturity improves cyber resilience by learning from incidents and through threat hunting, and by creating a safer, more empowering environment for women-owned businesses. Limited resources, lack of technical knowledge, awareness gaps, and institutional capacity gaps are especially relevant to female entrepreneurs. The project calls for the development of specialized training programs, forensics tools, and policies to build forensics capacity from the bottom up (for example, the Cyber Shakti or e-Safe HER projects in India). In conclusion, developing digital forensics maturity will play a key role in fostering an inclusive digital entrepreneurship environment. By addressing the security challenge, this approach will promote safer engagement in the digital realm, leading to sustainable development and gender equality.

***Keywords**: Digital Forensics Maturity, Cyber Resilience, Women Entrepreneurs, Forensic Readiness, Cybersecurity, Digital Safety, Women-Led SMEs.*

Introduction

"When a woman moves forward, the family moves, the village moves and the nation moves."

- Jawahar Lal Nehru

The digital economy has fundamentally reshaped modern entrepreneurship. Digital technologies such as e-commerce platforms, cloud computing, mobile banking, social media marketing, and remote collaboration tools have enabled entrepreneurs to scale businesses rapidly and reach global markets.

[*] *Copyright © 2026 by Author's and Licensed by Inspira. This is an open access article distributed under the Creative Commons Attribution License which permits unrestricted use, distribution, and reproduction in any medium, provided the original work properly cited.*

[*]***A Special Issue for the papers accepted for publication in the Two-Days Multidisciplinary National Seminar on Role of Entrepreneurship in Socio-Economic Upliftment of Women in India(22-23May 2026) Organized by Faculty of Commerce, The Graduate School College for Women, Jamshedpur, Jharkhand(A Constituent Unit of Kolhan University, Chaibasa, Jharkhand)in Collaboration with Jharkhand State Higher Education Council, Department of Higher and Technical Education, Govt. of Jharkhand & Punjab and Sind Bank, Sakchi, Jamshedpur.***

Women entrepreneurs have increasingly embraced digital entrepreneurship as a pathway for economic empowerment, financial independence, and social inclusion. Research on female digital entrepreneurship highlights that digital technologies reduce traditional barriers to business participation and facilitate flexible business operations.

Despite these opportunities, digital entrepreneurship introduces substantial cybersecurity challenges. Women entrepreneurs often manage resource-constrained businesses with limited access to cybersecurity expertise, advanced security infrastructure, and institutional support. As cyberattacks continue to increase globally, women-led enterprises have become vulnerable to cybercrime, including phishing attacks, account compromise, financial fraud, malware infections, and ransomware attacks. Recent empirical evidence from India indicates that approximately 66% of surveyed women entrepreneurs experienced cyber threats affecting business operations and customer trust.

Cyber resilience has therefore emerged as a critical organizational capability. Cyber resilience refers to the ability of organizations to anticipate, withstand, respond to, recover from, and adapt to cyber incidents. Organizations with mature cybersecurity and digital forensic capabilities are more capable of maintaining operational continuity during and after cyber incidents.

Digital forensics maturity represents an organization's level of preparedness to collect, preserve, analyse, and utilize digital evidence during cybersecurity incidents. Mature digital forensic systems improve incident response, facilitate legal compliance, support evidence preservation, and enhance post-incident learning. Studies on digital forensic readiness and maturity models emphasize the importance of proactive forensic preparedness for improving organizational resilience.

Objectives

The primary objectives of this review paper are:

- To review existing literature on digital forensics maturity and cyber resilience.
- To examine cybersecurity challenges affecting women entrepreneurs.
- To analyse the relationship between digital forensics maturity and organizational cyber resilience.
- To identify barriers limiting forensic readiness among women-led enterprises.
- To propose recommendations for improving cyber safety and resilience among women entrepreneurs.

Methodology

This study adopts a systematic narrative review methodology. Literature is collected from international and national journals, cybersecurity reports. This isfocused between 2020 and 2026 covering:

- Digital forensics maturity models
- Cybersecurity maturity frameworks
- Cyber resilience assessment
- Women entrepreneurship and digitalization
- Cybersecurity challenges among SMEs

Conceptual Foundations

- **Digital Forensics Maturity**

Digital forensics involves the systematic identification, collection, preservation, analysis, and presentation of digital evidence for investigative purposes. Digital forensic readiness extends this concept by emphasizing proactive preparation for future cyber incident.

Digital forensics maturity refers to the extent to which organizations institutionalize forensic capabilities within operational and governance structures. Maturity models typically assess organizational preparedness across multiple dimensions, including:

  - Governance and policy structures
  - Incident response capability
  - Evidence collection and preservation

- Technical infrastructure
- Legal and compliance readiness
- Employee awareness and training
- Continuous improvement mechanisms

The Digital Forensic Readiness and Maturity Model (DFMM) proposed by researchers extends forensic readiness frameworks to help organizations evaluate forensic preparedness and security incident response capabilities. Indicators of forensic maturity include:

- Existence of formal cybersecurity policies.
- Availability of forensic investigation procedures.
- Security monitoring systems.
- Employee cyber awareness programs.
- Digital evidence management practices.
- Regulatory compliance mechanisms

- **Cyber Resilience**

Cyber resilience refers to an organization's capability to continue operations despite cyber disruptions. Unlike traditional cybersecurity approaches focused primarily on prevention, cyber resilience emphasizes:

- Prevention
- Detection
- Response
- Recovery
- Adaptation

A systematic review of cyber-resilience frameworks found that resilient organizations integrate technological, organizational, and human-centred approaches to maintain continuity during cyber incidents. Cyber resilience includes:

- Rapid incident detection.
- Operational continuity.
- Data recovery capability.
- Organizational adaptability.
- Post-incident learning

Recent cybersecurity maturity studies indicate that organizations with structured maturity assessment systems demonstrate improved resilience outcomes and stronger alignment between security practices and business objectives.

- **Women Entrepreneurs in the Digital Economy**

Women entrepreneurs increasingly participate in digital entrepreneurship through online retailing, freelancing, digital services, fintech, social commerce, and platform-based business models. Literature reviews on female digital entrepreneurship highlight the transformative role of digital technologies in promoting financial inclusion and entrepreneurial participation among women. However, women entrepreneurs face unique barriers including:

- Limited access to capital
- Inadequate digital literacy
- Social and institutional constraints
- Limited cybersecurity awareness
- Insufficient technical support

Research on women-led digital enterprises emphasizes that cybersecurity vulnerabilities significantly threaten business sustainability and consumer trust.

Literature Review

- **Evolution of Digital Forensics Maturity Models**

Digital forensics maturity models evolved from broader capability maturity frameworks used in software engineering and information security governance. These models assess organizational preparedness using staged developmental levels.The literature identifies several major maturity dimensions:

- Policy and governance maturity
- Technical maturity
- Organizational maturity
- Legal and regulatory maturity
- Investigative capability maturity

Research on forensic readiness demonstrates that organizations often struggle to integrate forensic capabilities due to insufficient training, inadequate resources, and fragmented governance systems.

- **Cybersecurity Challenges Faced by Women Entrepreneurs**

Women entrepreneurs operating digital businesses face multiple cybersecurity risks:

- Phishing and credential theft
- Social engineering attacks
- Financial fraud
- Malware infections
- Ransomware attacks
- Data privacy breaches

Empirical studies conducted among women entrepreneurs in India found that cyber threats significantly affect operational continuity and customer trust. The study also revealed that implementation barriers include:

- High cybersecurity costs
- Lack of technical expertise
- Limited awareness of institutional support
- Resource constraints

Digital entrepreneurship literature further indicates that women-owned enterprises frequently prioritize business expansion over cybersecurity investment, thereby increasing organizational vulnerability.

- **Relationship Between Digital Forensics Maturity and Cyber Resilience**

Existing literature strongly suggests a positive relationship between forensic maturity and cyber resilience. Organizations with mature forensic capabilities demonstrate:

- Faster incident detection
- Efficient response coordination
- Improved evidence preservation
- Reduced operational downtime
- Better legal defensibility
- Enhanced recovery capability

Digital forensic readiness contributes to resilience by enabling organizations to identify root causes of cyber incidents and implement corrective measures. Research on cybersecurity as a dynamic organizational capability argues that resilience develops through continuous learning, adaptation, and socio-technical integration. This is particularly relevant for women entrepreneurs because:

- SMEs often lack dedicated cybersecurity departments
- Informal business structures increase risk exposure
- Resource limitations require adaptive resilience strategies

Consequently, digital forensic maturity acts as a resilience enabler by improving preparedness and organizational learning.

Limitation and Delimitation

- **Importance of Forensic Readiness for Women Entrepreneurs**

  Digital forensic readiness improves:

  - Incident response efficiency
  - Business continuity
  - Regulatory compliance
  - Customer trust
  - Legal preparedness

  Women entrepreneurs operating e-commerce and digital businesses benefit significantly from forensic readiness because online business models are highly dependent on data integrity and digital trust.

- **Barriers to Digital Forensics Maturity**

  Key barriers include:

  - Financial constraints
  - Limited cybersecurity expertise
  - Inadequate awareness
  - Insufficient government support
  - Lack of affordable forensic tools
  - Complex compliance requirements

- **Role of Institutional Support**

  Institutional support mechanisms are essential for improving cyber resilience among women entrepreneurs. Effective interventions include:

  - Cybersecurity awareness programs.
  - Subsidized forensic technologies.
  - Digital literacy training.
  - Mentorship initiatives.
  - Public-private cybersecurity partnerships.
  - Gender-sensitive cybersecurity policies can improve participation and resilience outcomes.

Gaps

The review identifies several research gaps:

- Limited empirical studies focusing specifically on women entrepreneurs and digital forensics maturity.
- Insufficient gender-sensitive cybersecurity frameworks.
- Lack of SME-oriented forensic readiness assessment models.
- Limited cross-country comparative studies.
- Inadequate integration of psychological and socio-cultural dimensions into resilience models.

Future studies should employ mixed-method and longitudinal approaches to validate relationships between forensic maturity and resilience outcomes.

Recommendations For Women Entrepreneurs

Women entrepreneurs should:

- Implement cybersecurity awareness training
- Use multi-factor authentication
- Maintain regular data backups
- Develop incident response procedures
- Conduct periodic security audits

Conclusion

The rapid expansion of digital entrepreneurship has created substantial opportunities for women entrepreneurs while simultaneously increasing exposure to cyber threats. This review paper demonstrates that digital forensics maturity significantly influences cyber resilience and organizational safety among women-led enterprises.

Organizations with mature forensic capabilities are better equipped to detect, investigate, respond to, and recover from cyber incidents. Digital forensic readiness improves operational continuity, strengthens customer trust, enhances legal preparedness, and supports sustainable business growth.

However, women entrepreneurs continue to face significant barriers, including financial limitations, inadequate technical expertise, and insufficient institutional support. Addressing these challenges requires collaborative efforts among governments, academic institutions, cybersecurity professionals, and entrepreneurial support organizations.

Future resilience strategies should prioritize inclusive cybersecurity ecosystems, lightweight maturity frameworks for SMEs, and gender-sensitive digital safety policies. As digital economies continue to evolve, digital forensics maturity will become increasingly essential for ensuring safe, resilient, and sustainable entrepreneurship among women worldwide.

References

1. "An Extended Digital Forensic Readiness and Maturity Model." *Forensic Science International: Digital Investigation*. (ScienceDirect)
2. "Indicators for Maturity and Readiness for Digital Forensic Investigation in Era of Industrial Revolution 4.0." *Computers & Security*. (ScienceDirect)
3. "A Systematic Review of Cyber-Resilience Assessment Frameworks." *Computers & Security*. (ScienceDirect)
4. "Recent Trends in Information and Cyber Security Maturity Assessment: A Systematic Literature Review." *Systems*. (MDPI)
5. "Cyber Threat Exposure and Institutional Support for Women Entrepreneurs in E-Commerce: A Study of Delhi and Faridabad." *International Journal on Research and Development – A Management Review*. (journals.mriindia.com)
6. "Female Digital Entrepreneurship: A Structured Literature Review." *International Journal of Entrepreneurial Behavior& Research*. (Emerald)
7. "Digital Innovation and Women's Entrepreneurship: Integrating Fragmented Literature Through a Stage-Contingent Lens." *Digital Business*. (ScienceDirect)
8. "Strategic Management in Digital Women Entrepreneurship: A Systematic Literature Review." *AMC Indian Journal of Entrepreneurship*. (indianjournalofmarketing.com)
9. "Digitalization Effects on Women Entrepreneurship and Sustainability: A Systematic Literature Review." *Nordic Journal of Media Management*. (AAU Journals)
10. "Cybersecurity as a Dynamic Capability: How Micro and Small Social Enterprises Build Digital Resilience." *Information Systems Frontiers*. (Springer)
11. "Cyber Security Maturity Assessment Framework for Technology Startups: A Systematic Literature Review." *IEEE Access*. (ResearchGate)
12. "Digital Forensics in the Age of Smart Environments: A Survey of Recent Advancements and Challenges." *arXiv*. (arXiv)
13. "Research Trends, Challenges, and Emerging Topics of Digital Forensics: A Review of Reviews." *arXiv*. (arXiv)
14. "Machine Learning in Digital Forensics: A Systematic Literature Review." *arXiv*. (arXiv)
15. "Exploring the Potential of Large Language Models for Improving Digital Forensic Investigation Efficiency." *arXiv*. (arXiv).

❑❑❑