International Journal of Science and Research (IJSR)
ISSN: 2319-7064
Impact Factor 2025: 7.089

Women's Role in Cyber-Secure Managerial Practices: Contributions and Challenges in Service Sector Organizations

Nita A. Sangale[1], Dr. Varsha N. Bhabad[2]

[1]Research Scholar, Assistant Professor, K.V.N Naik, Arts, Commerce, Science College, Nashik, India – 422002
Email: *nitasangle7[at]gmail.com*

[2]Research Guide, Institute of Management, Research & Technology (IMRT), Nashik, India – 422002
Email: *varsha.hembade[at]gmail.com,varsha_bhabad[at]gmail.com*

Abstract: ***In the era of rapid digitalization, cyber-secure managerial practices have become essential for protecting organizational data, systems, and decision-making processes. Service sector organizations-such as healthcare, education, banking, hospitality, and retail-depend heavily on women professionals who manage sensitive information, support digital workflows, enforce compliance policies, and facilitate security awareness among employees. This study examines the role of women in strengthening cyber-secure managerial practices using exclusively secondary data from industry reports, research articles, and cybersecurity frameworks. Findings indicate that women contribute extensively in areas such as data governance, documentation, audit readiness, employee training, ethical digital behavior, and frontline cyber-risk monitoring. However, their participation in strategic cybersecurity decision-making remains limited due to gender stereotypes, inadequate access to cyber-skilling, multitasking pressures, and underrepresentation in leadership. The paper concludes that empowering women through digital literacy, policy-level inclusion, and leadership opportunities can significantly enhance cyber governance and improve cyber resilience in service sector organizations.***

Keywords: Women Professionals, Service –sector organizations, data Security, digitalization, digital literacy, leadership inclusion, Gender & Cybersecurity

1. Introduction

The digital transformation of service sector industries has brought unprecedented efficiency, connectivity, and customer convenience. However, it has also heightened exposure to cyber threats such as data breaches, phishing attacks, identity theft, ransomware, and internal misuse of digital resources. As a result, organizations are increasingly shifting from purely technical cybersecurity measures to management-driven, policy-oriented, and behavior-focused cyber-secure managerial practices. These practices include data protection policies, cyber hygiene training, risk assessment, digital communication monitoring, cloud security protocols, and incident response coordination.

Women constitute a significant proportion of the workforce in service industries such as healthcare, education, banking, hospitality, HR services, and retail. In many of these domains, women are positioned in roles that manage sensitive information, customer interactions, administrative controls, digital record-keeping, and compliance documentation. Their natural strengths-such as attention to detail, discipline, communication ability, collaborative leadership, and adherence to organizational rules-make them key contributors to cyber-secure governance.

Despite their growing involvement, women's contributions to cyber-secure managerial practices often remain undervalued or underreported. Gender stereotypes that link cyber security with technical expertise frequently exclude women from cyber security leadership roles. Many women in administrative and managerial positions implement secure digital practices daily but are not formally recognized as contributors to organizational cyber security. Additionally, limited exposure to technical training, multitasking responsibilities, and lower representation in senior management reduce their influence on cyber policy formation. Understanding women's specific contributions and the challenges they face is therefore essential for strengthening cyber security governance in service sector organizations. This research paper—based entirely on secondary data—explores how women shape cyber-secure managerial practices, the types of practices they commonly engage in, and the barriers that limit their strategic participation. The study also provides recommendations to enhance women's involvement in cyber governance and build digitally resilient organizations.

2. Literature Review

Existing literature highlights the growing importance of human-centric and managerial approaches to cybersecurity. Studies by (Bada et al.) emphasize that cybersecurity awareness and behaviour play a crucial role in preventing cyber incidents, often more than purely technical controls. (Kshetri) underscores the need for cybersecurity governance that integrates managerial decision-making with risk management.

Research on gender and organizational governance indicates that women positively influence compliance culture, ethical practices, and risk monitoring in service sector organizations. (Sharma and Dash) found that gender-diverse managerial teams demonstrate stronger compliance orientation and reduced operational risk. International Labour Organization reports further suggest that women are increasingly engaged in digital roles but face structural barriers to leadership and technical up skilling.

Studies focusing on women in cyber security (Bagchi-Sen & Rao; Arul Seel & Jacob) reveal persistent gender stereotypes, limited access to training, and underrepresentation in senior cyber roles. However, these studies also recognize women's strengths in documentation, policy implementation, awareness training, and frontline risk identification. The present study builds upon this literature by specifically examining women's contributions to cyber-secure managerial practices in service sector organizations using a secondary-data approach.

Objectives of the Study

- To understand the concept and scope of cyber-secure managerial practices.
- To study the role of women in cyber-secure managerial practices in the service sector
- To identify the key cyber-secure practices where women contribute.
- To examine the challenges women, face in cyber-secure managerial roles.
- To suggest recommendations to enhance women's participation in cyber governance.

3. Methodology /Approach

The study is descriptive and analytical in nature and is based exclusively on secondary data. Data were collected from :

- Research articles from Scopus/Web of Science indexed journals
- Reports from NASSCOM, DSCI, MeitY (Government of India)
- Cyber security workforce reports
- Industry-based case studies
- Online databases, e-books, and organizational policy documents

Cyber-Secure Managerial Practices: A Conceptual Overview

Cyber-secure managerial practices refer to the policy-driven, supervisory, administrative, and behavior-oriented actions taken by managers to protect an organization's digital assets, information systems, and data-handling processes. These practices complement technical cyber security measures by creating a secure work culture and ensuring adherence to rules and protocols.

Key Conceptual Elements:

1) **Policy Formulation and Governance**
   Creating rules and guidelines related to data privacy, access control, digital communication, password management, device usage, and cloud security.
2) **Risk Assessment and Threat Management**
   Identifying vulnerabilities, conducting cyber audits, analyzing potential threats, and preparing crisis response strategies.
3) **Digital Hygiene and Employee Awareness**
   Training employees on safe digital practices such as avoiding phishing, managing passwords, preventing data leaks, and securely handling sensitive information.
4) **Monitoring and Compliance**
   Supervising whether employees follow cyber policies, maintaining audit logs, and ensuring compliance with IT Act, GDPR, or industry regulations.
5) **Incident Reporting and Response Coordination**
   Ensuring immediate communication during cyber incidents, coordinating with IT, legal, HR, and management teams, and documenting breaches.
6) **Secure Adoption of Digital Tools**
   Supporting the use of secure software, encrypted communication systems, and authenticated platforms.

In summary, cyber-secure managerial practices focus on people, policies, and processes and ensure that cybersecurity becomes a shared organizational responsibility.

Women's Role in Cyber-Secure Managerial Practices

Women in service sector organizations play a crucial and often overlooked role in strengthening cyber-secure work environments. Their contributions extend beyond technical functions and significantly influence organizational behaviour and policy compliance.

Key Roles Played by Women:

1) **Data Governance and Responsible Documentation**
   Women often handle sensitive HR, finance, and customer records, ensuring secure documentation and confidentiality.
2) **Compliance and Monitoring Leadership**
   Women frequently supervise adherence to data-protection rules, maintain audit records, and support risk assessment procedures.
3) **Training and Awareness Facilitation**
   Women excel in conducting cyber hygiene sessions, on boarding digital training, and communicating security guidelines to staff.
4) **Ethical Digital Behaviour Enforcement**
   Their natural strength in discipline, communication, and ethical conduct creates a secure and responsible digital culture.
5) **Frontline Cyber-Risk Identification**
   Women notice unusual activities, suspicious communication, and policy violations early due to strong observation skills.
6) **Secure Digital Workflow Management**
   In hospitals, schools, banks, and offices, women ensure secure digital record-keeping, safe customer interactions, and controlled access to information.

Types of Cyber-Secure Managerial Practices Women Contribute To

1) **Information and Data Protection Practices**
- Maintaining confidential HR and financial data
- Safe handling of customer documents

2) **Access Control and Authentication**
- Supervising login credentials
- Monitoring secure workplace entry and system access

3) **Digital Documentation Compliance**
- Maintaining audit trails
- Updating digital logs
- Ensuring accurate digital recordkeeping

4) **Employee Training and Awareness Programs**
- Cyber hygiene sessions

- Anti-phishing awareness
- Secure communication protocols

5) Cyber Risk Monitoring
- Identifying suspicious emails
- Reporting unauthorized activities
- Observing digital misuse

6) Secure Communication Practices
- Ensuring safe email use
- Preventing data leakage
- Promoting encrypted communication

7) Administrative Coordination during Cyber Incidents
- Documenting incidents
- Coordinating with IT and management
- Ensuring follow-up action

Challenges Faced by Women in Cyber-Secure Managerial Practices

1) Gender Stereotyping in Cybersecurity
   Cybersecurity is viewed as a technical field, often excluding women from decision-making roles.
2) Limited Access to Cyber Skills Training
   Women receive fewer opportunities for upskilling compared to men.
3) Underrepresentation in Leadership
   Few women are in senior managerial or cybersecurity governance positions.
4) Work–Life Balance and Multitasking Pressure
   Heavy workloads restrict the time available for cybersecurity learning.
5) Lack of Confidence in Technical Discussions
   Social conditioning sometimes lowers women's confidence in tech-related meetings.
6) Cyber Harassment and Digital Safety Risks
   Women face higher vulnerability to phishing, social engineering, and online harassment.
7) Recognition Gap
   Women perform vital compliance and documentation tasks but rarely receive acknowledgment.

4. Data Analysis

Secondary data analysis reveals that a significant proportion of cybersecurity incidents in service sector organizations arise due to human error, weak policy compliance, and lack of awareness rather than technical failures. It further also indicate that documentation lapses, insecure communication, and inadequate training contribute substantially to cyber risk.

Industry and workforce studies show that women are predominantly engaged in administrative, HR, compliance, and operational management roles where cyber-secure practices such as data handling, audit maintenance, access control, and employee awareness are critical. Organizations with higher representation of women in these roles demonstrate stronger compliance mechanisms and lower instances of policy violations.

The analysis also highlights a gap between operational contribution and strategic participation. While women actively implement cyber-secure practices, they remain underrepresented in cybersecurity governance committees, policy formulation teams, and strategic decision-making bodies. Limited access to advanced cybersecurity training further restricts their upward mobility into leadership roles

5. Findings

- Women significantly contribute to operational and managerial cybersecurity functions in service sectors.
- Their strengths-attention to detail, communication, compliance orientation— improve organizational cyber hygiene.
- Women play important roles in training, documentation, data governance, and risk monitoring.
- Gender stereotypes restrict women's participation in strategic cybersecurity planning.
- Many service sector organizations do not formally recognize women's cybersecurity contributions.
- Lack of structured digital-skilling programs limits women's growth in cybersecurity roles.
- Organizations with more women in administrative posts show higher compliance levels and lower human-error-based cyber incidents.

6. Recommendations

1) Provide Cybersecurity Training for Non-Technical Women Staff
   Beginner-friendly digital security training should be compulsory.
2) Increase Women's Representation in Cyber Governance Committees
   Include women in data-protection teams, cyber policy meetings, and audit boards.
3) Break Gender Stereotypes Through Organization-Wide Awareness
   Promote cybersecurity as a managerial—not purely technical—responsibility.
4) Implement Mentorship and Leadership Programs
   Create pathways for women to grow into cyber governance leadership.
5) Strengthen Digital Policies Related to Women's Safety
   Provide support systems for cyber harassment reporting.
6) Encourage Flexible Work Arrangements
   To balance multitasking pressures and support continuous learning.
7) Reward and Recognize Women's Cyber Contributions
   Include cybersecurity performance in appraisal systems.

7. Conclusion

Women play a transformative role in strengthening cyber-secure managerial practices in service sector organizations. Their contributions in data governance, compliance, training, ethical conduct, and risk monitoring are critical for building cyber resilience. Despite these contributions, women continue to face barriers such as gender biases, limited training access, and underrepresentation in leadership. Empowering women through skill development, inclusive policies, and leadership opportunities can significantly enhance the cyber governance capacity of service institutions. A digitally skilled and gender-inclusive workforce is essential for secure, efficient, and future-ready service sector organizations.

References

[1] Bada, M., Sasse, A. M., & Nurse, J. R. C. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? Cyber Security, 2(1), 1–14. https://doi.org/10.1186/s42400-019-0030-1
[2] Cummings, T. G., & Worley, C. G. (2020). Organization development and change (11th ed.). Cengage Learning.
[3] Data Security Council of India. (2022). Cyber security workforce demand and skill gap analysis. DSCI.
[4] Dutta, S., Lanvin, B., & Wunsch-Vincent, S. (2023). Global cybersecurity index. World Economic Forum.
[5] Government of India. (2000). Information Technology Act, 2000. Ministry of Law and Justice.
[6] International Labour Organization. (2022). Women and digital transformation in service sector employment. ILO.
[7] Kshetri, N. (2021). Cybersecurity management: A review and future research agenda. Journal of Global Information Technology Management, 24(3), 1–15. https://doi.org/10.1080/1097198X.2021.1930822
[8] NASSCOM. (2023). Cybersecurity in India: Building a resilient digital ecosystem. National Association of Software and Service Companies.
[9] OECD. (2020). Digital security risk management for economic and social prosperity. OECD Publishing.
[10] PwC. (2022). Global digital trust insights survey. PricewaterhouseCoopers.
[11] Sharma, R., & Dash, S. (2021). Gender diversity and organizational compliance culture in service industries. International Journal of Human Resource Management, 32(12), 2564–2585. https://doi.org/10.1080/09585192.2020.1737834
[12] Singh, A., & Gupta, P. (2020). Role of women managers in organizational governance and compliance. Asian Journal of Management Research, 10(2), 45–58.
[13] World Economic Forum. (2022). Global risks report: Cyber insecurity and human factor. WEF.
[14] Bagchi-Sen, S., & Rao, R. (2010). Women in cybersecurity: A study of career advancement. IT Professional, 12(1), 24–31. https://doi.org/10.1109/MITP.2010.39
[15] Arul Seel, L., & Jacob, R. (2024). The role and challenges of women in cybersecurity in Nagapattinam District, Tamil Nadu, India. Scientific Culture, 10(1), 611–624.
[16] A study of female cybersecurity professionals. (2023). Issues in Information Systems, 24(3), 83–96. https://doi.org/10.48009/3_iis_2023_108
[17] Deshmukh, R. K. (2024). Cyber security concerns for women in the digital era. ITIHAS DARPAN Conference Proceedings (Special Issue, October 2024).