Journal of Engineering Issues and Solutions

Cyber Defense Readiness and Adoption Barriers among Small and Medium-Sized Businesses in Nepal: A Mixed-Methods Study

Yam Krishna Poudel[1*], Kamana Pokharel[2], Sagar Bastola[3]

[1]Department of Electrical & Electronics, Nepal Engineering College, Pokhara University, Nepal -yampd01@gmail.com
[2]Ace college of Management, Kathmandu Nepal Affiliated to Pokhara University, Kamanapkhl@gamil.com
[3]Himalayan College of Management, Kathmandu, Nepal Affiliated with Infrastructure University Kuala Lumpur, Malaysia
**Corresponding email: Yam Krishna Poudel -yampd01@gmail.com*
Received: May 12, 2026; Revised: 13 June, 2026; Accepted: July 11, 2026

Abstract

Small and medium-sized businesses (SMBs) are key drivers of Nepal's growing digital economy, yet their cybersecurity readiness remains underexplored. This study assesses the organizational preparedness of Nepalese SMBs by examining cybersecurity awareness, organizational practices, training, incident experience, and confidence in mitigating cyber threats. A mixed-methods research design was adopted, combining a structured questionnaire administered to 150 stakeholders representing SMBs with semi-structured interviews to enrich the interpretation of quantitative findings. The survey instrument demonstrated good internal reliability (Cronbach's alpha = 0.82). The findings reveal that cybersecurity preparedness is primarily constrained by low awareness, limited organizational resources, budget limitations, and insufficient technical expertise, which together constitute the dominant barriers to effective cybersecurity implementation. Regular cybersecurity training remains inadequate across many organizations, while reported cyber incidents increase with organizational size. Furthermore, confidence in preventing cyber threats is generally low, indicating significant gaps between perceived risks and organizational preparedness. Interpreted through the Technology Organization Environment (TOE) framework, the results suggest that cybersecurity readiness is influenced more by organizational capacity, resource availability, and institutional support than by the sophistication of cyber threats alone. Based on these findings, the study proposes a practical four-stage cybersecurity maturity roadmap, Govern and Baseline, Protect Essentials, Detect and Respond, and Optimize and Collaborate, aligned with the NIST Cybersecurity Framework (CSF) 2.0 and Nepal's National Cyber Security Policy. The proposed framework provides a scalable, resource-sensitive approach to strengthening cyber resilience among Nepalese SMBs and offers practical guidance for business leaders, policymakers, and cybersecurity practitioners seeking to enhance organizational security in resource-constrained environments.

Keywords: *cybersecurity; small and medium-sized businesses; Nepal; cyber resilience; training; technology adoption; TOE framework*

1. Introduction

Digital transformation has expanded the market reach, speed, and operational efficiency of smaller firms, but the same transition has also created new points of cyber exposure. As businesses become more dependent on connected systems and digital services, they face a wider range of threats, including phishing, malware, ransomware, credential theft, service disruption, and data loss (Alahmari & Duncan, 2020; Saeed et al., 2023).

These risks are particularly difficult for SMBs because technology adoption often advances faster than security governance and organizational capacity. Many firms operate without dedicated security personnel, formal risk-management processes, reliable monitoring, or tested response plans; consequently, cybersecurity becomes not only a technical challenge but also a matter of leadership, employee behavior, financial prioritization, and access to specialist expertise (Chaudhary et al., 2023; van Haastrecht et al., 2021).

The Nepalese context makes this challenge increasingly urgent as firms rely more heavily on online banking, digital payment systems, cloud services, social media, customer databases, and remote collaboration tools. Although Nepal's National Cyber Security Policy emphasizes resilience, institutional coordination, capacity building, and the protection of digital infrastructure, implementation remains uneven among businesses with limited financial and technical resources (Ministry of Communication and Information Technology [MoCIT], 2023).

Empirical evidence on cyber readiness among Nepalese SMBs remains limited, which weakens the ability of policymakers, industry associations, and service providers to design interventions that are both affordable and proportionate. To address this gap, the present study examines five connected dimensions: firm-size profile, perceived adoption barriers, training frequency, incident experience, and confidence in prevention, before integrating the results through the technology-organization-environment (TOE) framework.

This research study makes two related contributions. It first provides a transparent descriptive account of cyber-defense readiness across a diverse sample of Nepalese SMBs and then translates that evidence into a staged implementation roadmap, beginning with governance and essential controls before introducing advanced monitoring at higher levels of operational maturity.

2. Literature Review and Conceptual Foundation

2.1 Cybersecurity Readiness in SMBs

SMBs commonly implement basic antivirus, firewall, backup, and patching practices, yet they are less likely to maintain structured awareness programs, formal risk assessment, centralized logging, incident-response exercises, or dedicated security staff (European Union Agency for Cybersecurity [ENISA], 2021). Technical controls are necessary but insufficient. Owners allocate budgets and establish risk appetite, managers translate policy into routines, employees handle credentials and sensitive data, IT personnel configure systems, and external providers frequently supply expertise that cannot be sustained internally (Antunes et al., 2021; Bada & Nurse, 2019).

Advanced intrusion detection and machine-learning tools can improve pattern recognition, but their value depends on reliable data, integration capacity, maintenance, and skilled interpretation. Deployment studies warn that model drift, false positives, poor data quality, and operational complexity can outweigh benefits where basic security controls remain immature (Paleyes et al., 2022; Rawindaran et al., 2021). A readiness-oriented strategy should therefore prioritize usable controls and organizational routines before advanced analytics.

2.2 TOE Framework

The TOE framework explains technology adoption through three interacting contexts: technology, organization, and environment (Tornatzky & Fleischer, 1990). In cybersecurity, the technology context includes affordability, complexity, compatibility, and perceived benefit; the organizational context includes leadership, skills, financial capacity, firm size, and security culture; and the environmental context includes policy, standards, vendor support, competitive pressure, and external expertise. The extended TOE perspective is appropriate for cybersecurity because adoption responds simultaneously to technological options, internal capability, threat catalysts, and institutional expectations (Wallace et al., 2020).

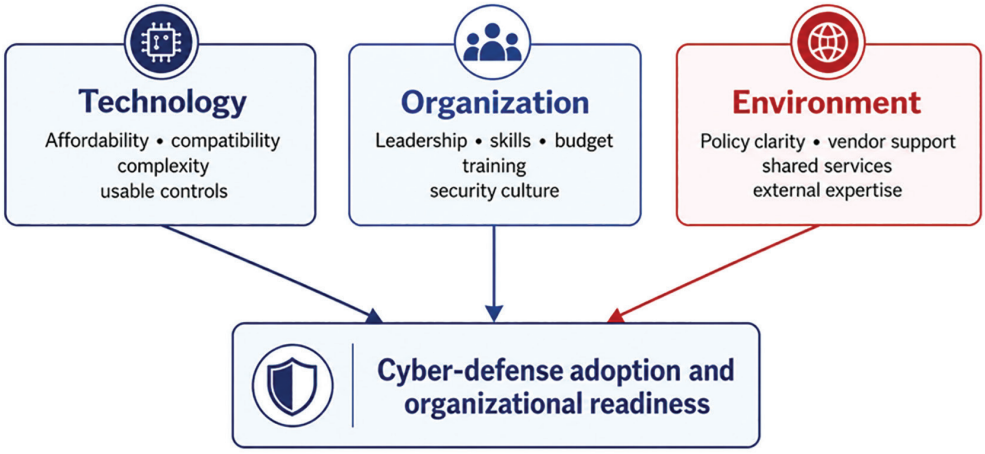

Figure 1: TOE-informed framework for interpreting cyber-defense adoption and readiness in Nepalese SMBs.

3. Methodology

3.1 Design, Participants, and Analytical Base

This Research paper used a mixed-methods design combining a structured online survey with semi-structured interviews. Survey invitations were distributed through email, social media, and professional networks to firms from IT and software, finance, health, manufacturing, retail, hospitality, and related sectors. A total of 225 questionnaires were distributed and 151 responses were reported, producing a 67.1% response rate. 150 responded are used for research study.

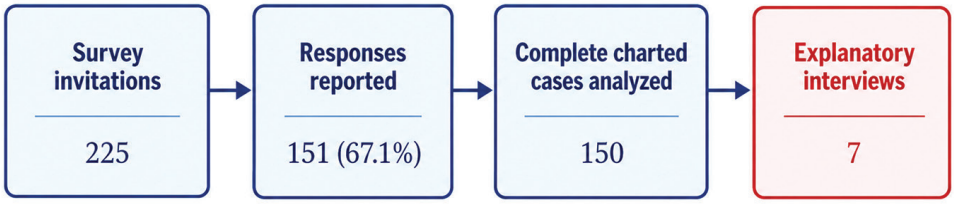

Figure 2: Mixed-methods sample and analytical flow. The quantitative analysis uses the 150 complete charted cases.

Table 1: Study design and analytical base.

Element	Reported value	Use in this article
Survey invitations	225	Distributed through Nepalese SMB networks
Responses reported	151	Response rate = 67.1%
Complete charted observations	150	complete response
Interviews	7	
Internal consistency	Cronbach's α = .82	

3.2 Measures, Analysis, and Research Quality

The questionnaire covered organization size, respondent role, existing controls, training frequency, perceived barriers, incident experience during the previous 12 months, prevention confidence, and preferred forms of external support. Organization size was categorized as micro (1–10 employees), small (11–50), and medium (51–250). Quantitative analysis was descriptive

4. Results

4.1 Organization Profile

Micro firms formed the largest group (n = 69, 46.0%), followed by small firms (n = 50, 33.3%) and medium firms (n = 31, 20.7%). Thus, 79.3% of the sample consisted of micro or small businesses. This profile is suitable for examining resource constraints, although the smaller medium-business subgroup requires cautious interpretation of size comparisons. Organization size distributions are as shown in figure 3.

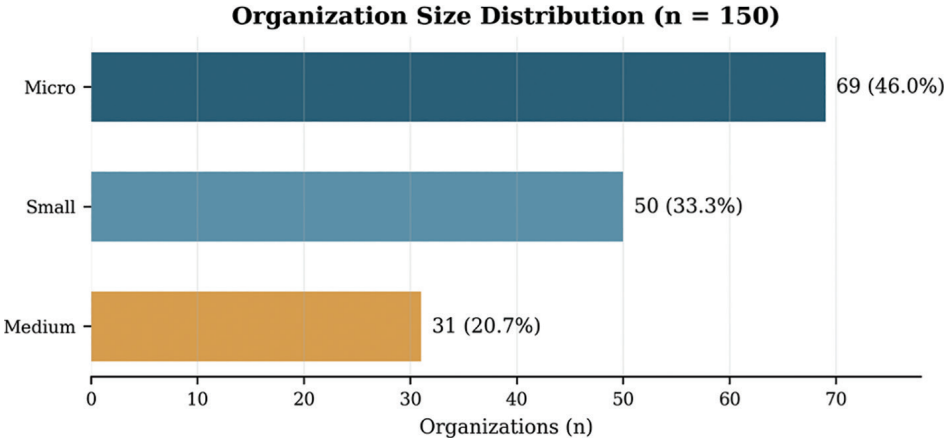

Figure 3: Organization size distribution in the complete charted sample (n = 150).

4.2 Primary cybersecurity barriers

Lack of awareness was the most frequently reported primary challenge (n = 37, 24.7%), closely followed by lack of resources (n = 35, 23.3%). Budget constraints accounted for 20.7% (n = 31), lack of expertise for 19.3% (n = 29), and increasing threat sophistication for 12.0% (n = 18). Awareness, resources, budget, and expertise together represented 88.0% of responses, demonstrating that foundational capability gaps outweighed concerns about advanced threat complexity as shown in figure 4.

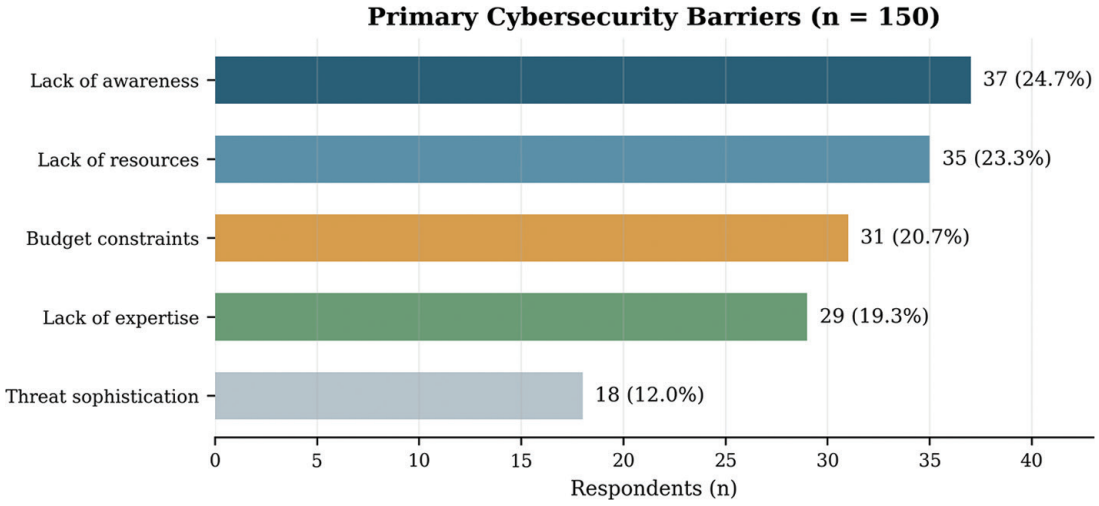

Figure 4: Primary cybersecurity barriers

4.3 Training frequency

Cybersecurity training was absent in 62 organizations (41.3%). Forty-five organizations (30.0%) trained once a year, 28 (18.7%) trained twice a year, and only 15 (10.0%) trained quarterly. Overall, 71.3% provided no training or only one session per year. This frequency is inadequate for recurring behavioral risks such as phishing, unsafe credential practices, social engineering, insecure data handling, and delayed incident escalation as shown in figure 5.

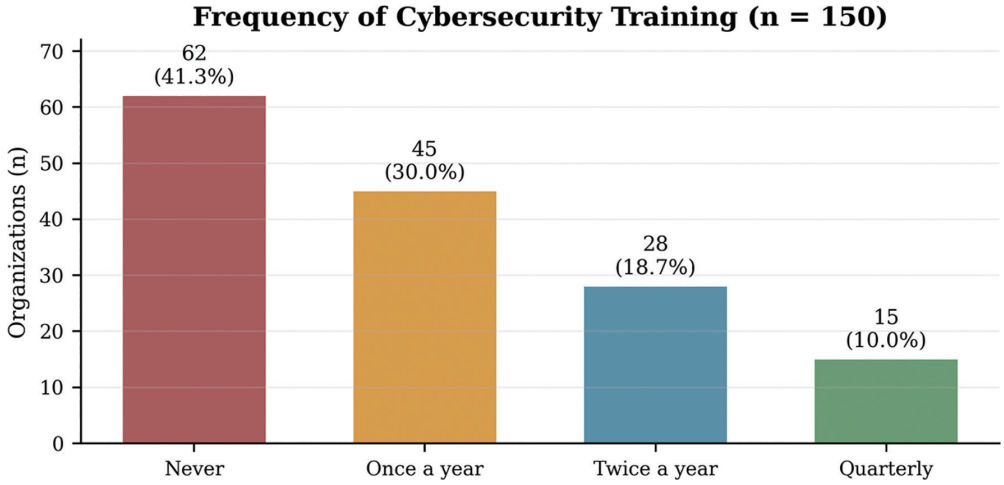

Figure 5: Frequency of cybersecurity training among surveyed organizations

4.4 Incident reporting by organization size

Sixty-two organizations (41.3%) reported a cybersecurity incident during the previous 12 months. Micro firms recorded 25 incidents among 69 organizations (36.2%; 95% CI 25.9%–48.0%), small firms recorded 21 among 50 (42.0%; 95% CI 29.4%–55.8%), and medium firms recorded 16 among 31 (51.6%; 95% CI 34.8%–68.0%). Contrary to the original dissertation narrative, the reported counts indicate the highest proportional incident rate among medium firms. This may reflect greater digital exposure, more complex

operations, stronger detection, or a combination of these factors; overlapping confidence intervals and the cross-sectional design prevent stronger conclusions as shown in figure 6.

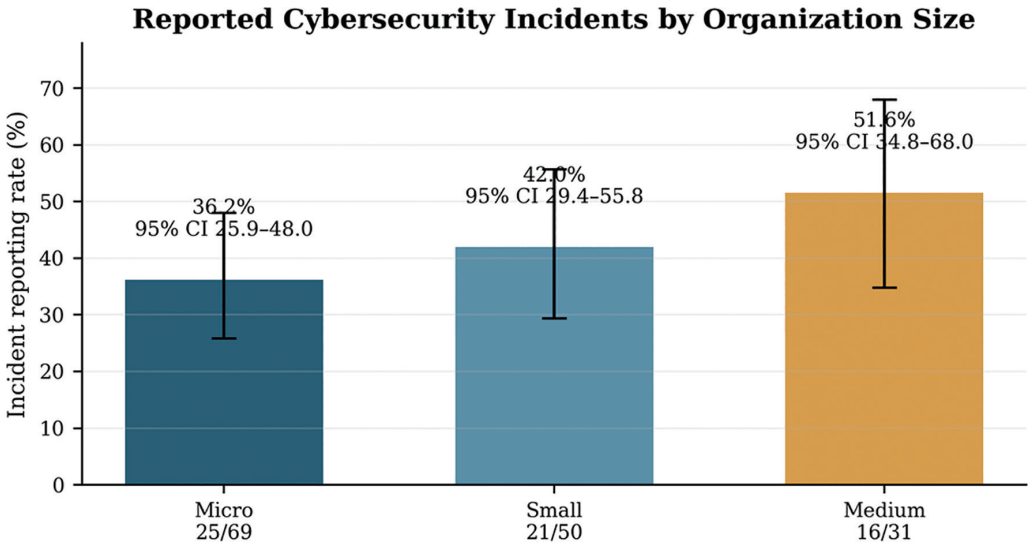

Figure 6: Reported incident rates by organization size with Wilson 95% confidence intervals.

4.5 Confidence in prevention by organizational role

Across all roles, 52 respondents (34.7%) were neutral, 44 (29.3%) were not confident, 42 (28.0%) were somewhat confident, and only 12 (8.0%) were very confident. Very-confident responses were uncommon in every group. Owners and executives reported the largest number of very-confident responses (n = 5), but they also included 13 not-confident respondents. IT managers were not uniformly confident: 16 were neutral, 9 not confident, 11 somewhat confident, and 2 very confident. The distribution does not support a simple assumption that technical roles are consistently more confident; instead, it indicates dispersed readiness and unclear shared responsibility as shown in figure 7.

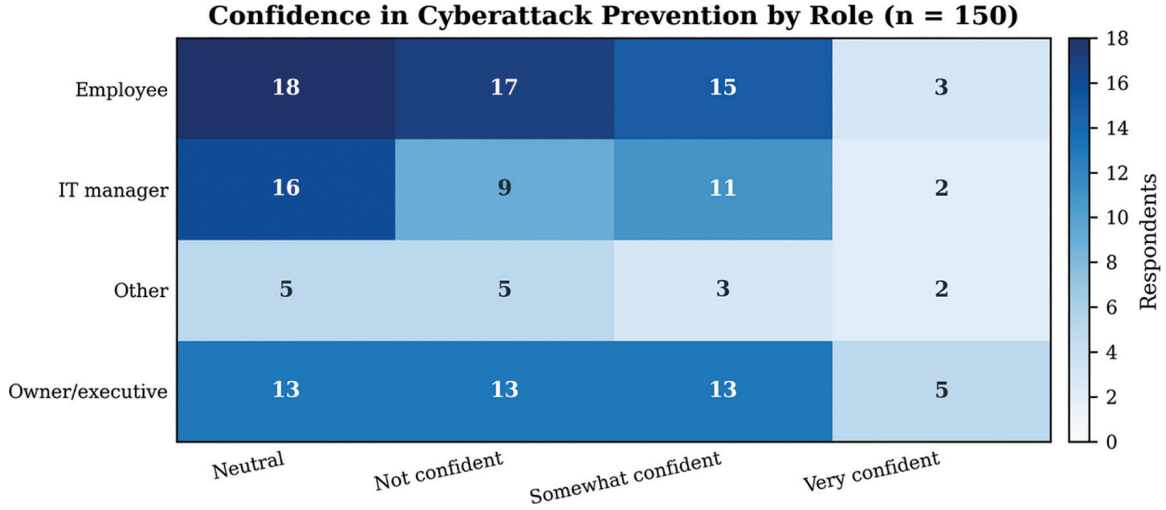

Figure 7: Prevention confidence by organizational role. Cell values are respondent counts (n = 150).

4.6 Integrated mixed-methods interpretation

The descriptive indicators converge on a consistent readiness gap: foundational barriers dominate, training is infrequent, incident experience is common, and strong prevention confidence is rare. The interviews reinforce these patterns by emphasizing scarce internal expertise, dependence on external providers, low policy awareness, and the need for affordable support. Figure 8 summarizes the principal quantitative signals, while Table 2 presents a mixed-methods joint display linking survey evidence, interview themes, and practical implications as shown in figure 8.

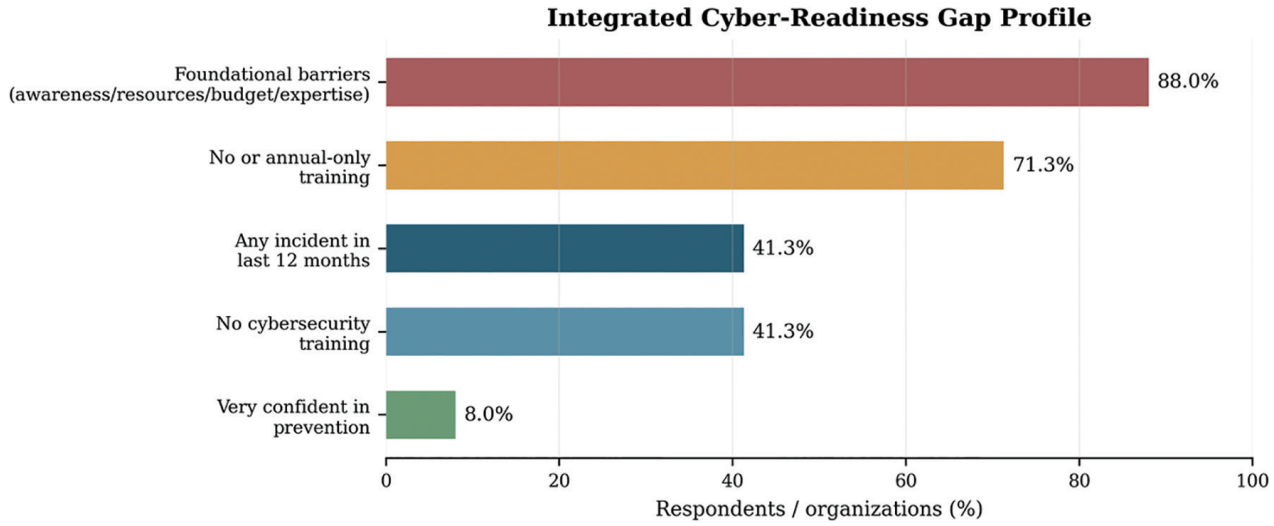

Figure 8: Integrated cyber-readiness gap profile

Table 2: Mixed-methods joint display of readiness signals and implications.

Survey signal	Interview-supported theme	Integrated implication
Foundational barriers = 88.0%	Limited resources, expertise, and affordable options	Prioritize basic capability and usable controls before advanced tools
No/annual-only training = 71.3%	Training is irregular and often generic	Use short, repeated, role-specific learning and exercises
Any incident = 41.3%	Detection and reporting capacity varies	Improve logging, escalation, and managed support
Very confident = 8.0%	Responsibility is fragmented across roles	Assign an accountable security owner and management metrics
Demand for external support	Dependence on consultants and vendors	Develop pooled services, vouchers, and sector-level assistance

5. Discussion

5.1 Technology context: usable foundations before advanced analytics

Affordability, compatibility, complexity, and perceived benefit define the technology context. The results show that Nepalese SMBs are constrained primarily by awareness, resources, budgets, and expertise rather than by the theoretical sophistication of cyber threats. Immediate priorities should therefore include asset inventories, secure configuration, patching, multifactor authentication, tested backups, endpoint protection,

email filtering, basic logging, and a documented incident contact process. These controls create the data quality and operational discipline required before advanced detection becomes useful. The NIST Cybersecurity Framework 2.0 Small Business Quick-Start Guide similarly emphasizes progressive governance, identification, protection, detection, response, and recovery (Eliot, 2024).

When intrusion detection or managed monitoring is adopted, deployment should be proportionate. Micro firms may gain more value from vendor-supported endpoint detection, cloud-native logging, and managed services than from maintaining an on-premise machine-learning platform. Small and medium firms with more complex networks can gradually introduce segmentation, centralized alerts, and higher-level analytics. This interpretation is consistent with evidence that advanced cybersecurity adoption in SMEs depends on cost-benefit clarity, compatible infrastructure, and access to specialist expertise (Rawindaran et al., 2021).

5.2 Organizational context: leadership, training, and shared responsibility

The organizational context is the strongest empirical signal. More than two-fifths of organizations never conducted cybersecurity training, and only 8.0% of respondents were very confident in prevention. Cyber risk is therefore not yet embedded in routine management. Training should move from occasional presentations to short, repeated, role-specific activities: phishing recognition for all staff, privileged-access practices for administrators, payment verification for finance personnel, breach escalation for managers, and business continuity exercises for owners. Effective awareness programs connect guidance to daily work rather than deliver generic information (Bada & Nurse, 2019).

Leadership must convert awareness into accountability. A designated security owner—even as a part-time responsibility—should maintain a simple risk register, confirm backup testing, monitor training completion, review high-risk vendors, and coordinate incident reporting. Decision-makers need understandable metrics such as multifactor-authentication coverage, patch status, backup restoration success, phishing-reporting rates, unresolved critical alerts, and time to contain incidents. Socio-technical measures are more useful to SMBs than purely technical dashboards because they link controls to people and business processes (van Haastrecht et al., 2021).

5.3 Environmental context: policy translation and shared services

Nepal's national policy provides strategic direction, but SMBs require operational translation: minimum control baselines, sector-specific checklists, simplified incident-reporting guidance, model vendor clauses, local-language awareness materials, and affordable assessment pathways. Government agencies, business associations, banks, insurers, internet service providers, universities, and cybersecurity firms can reduce adoption costs by pooling training and technical services. Subsidized baseline assessments or vouchers would directly address the resource and expertise barriers identified in the survey.

A shared service model is particularly appropriate where individual firms cannot employ dedicated security teams. Sector associations can procure managed monitoring, vulnerability assessments, incident-response retainers, and awareness platforms for members. Such arrangements improve bargaining power, standardization, and escalation pathways while allowing controls to scale according to risk. International evidence similarly indicates that SMEs benefit from structured external support and practical implementation assistance (Antunes et al., 2021; ENISA, 2021).

5.4 Staged cyber-resilience roadmap

The integrated findings support a four-stage roadmap. Stage 1 assigns accountability, inventories critical

assets, identifies obligations, maps suppliers, and establishes a baseline risk register. Stage 2 secures essential systems through multifactor authentication, patching, endpoint protection, least privilege, encryption, secure email, and tested offline or immutable backups. Stage 3 centralizes logs, defines incident categories, creates an internal and external contact tree, conducts tabletop exercises, and introduces managed detection where justified. Stage 4 measures performance, tests restoration and response, reviews vendors, shares threat information, and evaluates advanced analytics only when data, skills, and operational maturity are sufficient.

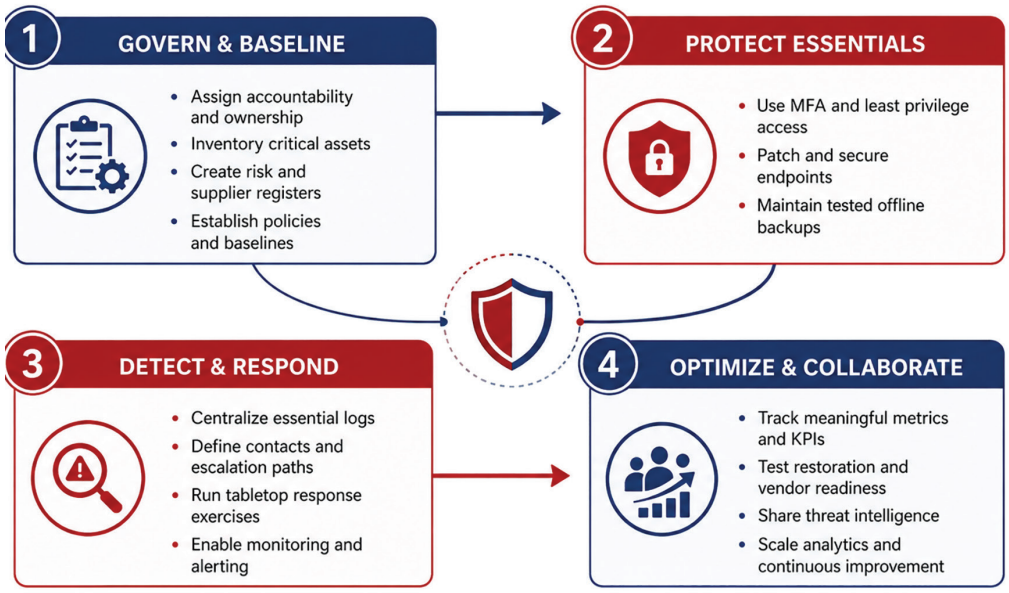

Figure 9: Four-stage cyber-resilience roadmap for resource-constrained Nepalese SMBs.

6. Implications, Limitations, and Future Research

6.1 Practical and policy implications

Business leaders should fund recurring foundational capability rather than isolated products. Regular expenditure on training, patching, backup testing, and expert support is likely to provide greater value than an advanced platform that cannot be operated effectively. Service providers should offer transparent tiered packages with clear responsibilities, local support, measurable service levels, and realistic escalation arrangements. Government and business associations should pair policy communication with minimum baselines, incentives, pooled services, local-language resources, and simplified reporting mechanisms.

6.2 Future research

Future studies should adopt stratified sampling across provinces and sectors so that organizational and regional variation can be examined more systematically. Firm-size categories should be applied consistently, and anonymized item-level data should be made available whenever ethical, legal, and confidentiality safeguards permit. Measurement quality could be strengthened by using validated multi-item scales that assess awareness, governance, technical maturity, incident-response capability, and environmental support as distinct constructs. Longitudinal research should then examine whether repeated training, subsidized assessments, or managed-security services produce measurable reductions in incident frequency, disruption, and recovery time. Future work should also combine management surveys with objective technical evidence, including vulnerability scans, configuration reviews, backup-restoration tests, incident logs, phishing

simulations, and vendor-risk assessments. Such triangulation would make it possible to quantify the difference between perceived readiness and observed security performance.

7. Conclusion

Nepalese SMBs face a cyber-defense problem rooted primarily in organizational capability and enabling conditions. Awareness deficits, limited resources, budget constraints, and lack of expertise dominate the reported barriers; training is infrequent; incident experience is substantial; and strong prevention confidence is rare. Corrected size-specific analysis indicates the highest proportional incident reporting among medium firms, challenging the assumption that micro firms are necessarily the most incident-prone. Interpreted through the TOE framework, the evidence supports a staged strategy that begins with governance and essential controls, strengthens training and shared responsibility, expands detection and response through affordable services, and introduces advanced analytics only when operational maturity is sufficient. Coordinated action by firms, government, business associations, financial institutions, universities, and cybersecurity providers is necessary to convert national policy direction into practical resilience.

Acknowledgements

The authors sincerely acknowledge the Ministry of Communication and Information Technology, Government of Nepal, for its support and the organizations and institutions that facilitated this research. We are grateful to all participating organizations, individual researchers, and respondents for their valuable cooperation during data collection. The authors also express their sincere appreciation to the faculty members and researchers from Tribhuvan University (TU) and Kathmandu University (KU) for their valuable guidance, constructive suggestions, and academic support throughout this study.

Declarationof Generative AI and AI-Assisted Technologies in the Writing Process

During the preparation of this manuscript, generative AI and AI-assisted technologies were used solely for language editing, grammar correction, paraphrasing, and improving readability. All scientific content, analyses, interpretations, conclusions, and recommendations were independently developed, verified, and approved by the authors, who accept full responsibility for the published work.

Conflicts of Interest

The authors declare that they have no known competing financial, professional, or personal interests that could have influenced the research reported in this paper.

Funding

This research received no external funding.

References

Alahmari, A., & Duncan, B. (2020). Cybersecurity risk management in small and medium-sized enterprises: A systematic review of recent evidence. In 2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA) (pp. 1–5). IEEE. https://doi.org/10.1109/CyberSA49311.2020.9139638

Antunes, M., Maximiano, M., Gomes, R., & Pinto, D. (2021). Information security and cybersecurity management: A case study with SMEs in Portugal. Journal of Cybersecurity and Privacy, 1(2), 219–238. https://doi.org/10.3390/jcp1020012

Bada, M., & Nurse, J. R. C. (2019). Developing cybersecurity education and awareness programmes for small- and medium-sized

enterprises (SMEs). Information & Computer Security, 27(3), 393–410. https://doi.org/10.1108/ICS-07-2018-0080

Chaudhary, S., Gkioulos, V., & Katsikas, S. (2023). A quest for research and knowledge gaps in cybersecurity awareness for small and medium-sized enterprises. Computer Science Review, 50, 100592. https://doi.org/10.1016/j.cosrev.2023.100592

Creswell, J. W. (2014). Research design: Qualitative, quantitative, and mixed methods approaches (4th ed.). SAGE.

Eliot, D. (2024). NIST Cybersecurity Framework 2.0: Small Business Quick-Start Guide (NIST SP 1300). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.1300

European Union Agency for Cybersecurity. (2021). Cybersecurity for SMEs: Challenges and recommendations. https://www.enisa.europa.eu/publications/enisa-report-cybersecurity-for-smes

Ministry of Communication and Information Technology. (2023). National Cyber Security Policy, 2080. Government of Nepal. https://mocit.gov.np/content/7119/7119-national-cyber-security-policy/

Paleyes, A., Urma, R.-G., & Lawrence, N. D. (2022). Challenges in deploying machine learning: A survey of case studies. ACM Computing Surveys, 55(6), Article 114. https://doi.org/10.1145/3533378

Rawindaran, N., Jayal, A., & Prakash, E. (2021). Machine learning cybersecurity adoption in small and medium enterprises in developed countries. Computers, 10(11), 150. https://doi.org/10.3390/computers10110150

Rawindaran, N., Jayal, A., Prakash, E., & Hewage, C. (2021). Cost benefits of using machine learning features in NIDS for cyber security in UK small medium enterprises (SME). Future Internet, 13(8), 186. https://doi.org/10.3390/fi13080186

Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023). Digital transformation and cybersecurity challenges for businesses resilience: Issues and recommendations. Sensors, 23(15), 6666. https://doi.org/10.3390/s23156666

Tornatzky, L. G., & Fleischer, M. (1990). The processes of technological innovation. Lexington Books.

van Haastrecht, M., Yigit Ozkan, B., Brinkhuis, M., & Spruit, M. (2021). Respite for SMEs: A systematic review of socio-technical cybersecurity metrics. Applied Sciences, 11(15), 6909. https://doi.org/10.3390/app11156909

Wallace, S., Green, K. Y., Johnson, C., Cooper, J., & Gilstrap, C. (2020). An extended TOE framework for cybersecurity-adoption decisions. Communications of the Association for Information Systems, 47, 338–363. https://doi.org/10.17705/1CAIS.04716