JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

CYBER DEFENSE CHALLENGES: A PERSPECTIVE FROM SMALL AND MEDIUM-SIZED BUSINESSES IN NEPAL

Yam Krishna Poudel

Asst.prof at Nepal Engineering College, Pokhara University, Nepal

Abstract

Cybersecurity has become a critical concern for small and medium-sized businesses (SMBs) in Nepal as they increasingly adopt digital technologies to enhance operations. However, these organizations often lack the resources, expertise, and infrastructure necessary to address emerging cyber threats. This research investigates the challenges SMBs face in implementing effective cyber defense strategies, emphasizing the unique vulnerabilities of these businesses. A mixed-methods approach was adopted, combining quantitative surveys and qualitative interviews. Surveys were conducted among 151 SMBs across various sectors, and interviews were held with business owners, IT managers, and cybersecurity professionals to identify key challenges. Findings indicate that limited financial resources, lack of awareness, and inadequate training are the primary barriers to implementing robust cybersecurity measures. Micro and small businesses, in particular, reported frequent cyber incidents but struggled with underreporting and minimal defensive preparedness. The study concludes with actionable recommendations, including government policy interventions, affordable cybersecurity tools, and targeted training programs to enhance SMBs' cyber defense posture. These insights aim to contribute to a more secure digital ecosystem for Nepal's growing business sector.

Keywords

Cybersecurity, Small and Medium-Sized Businesses (SMBs), Cyber Defense, Cyber Threats, Digital Vulnerability, Risk Management.

I. Introduction

Small and Medium-Sized Businesses (SMBs) are vital contributors to economic growth, employment, and innovation, especially in developing economies like Nepal. As digital transformation accelerates, SMBs increasingly rely on digital tools, cloud systems, and online platforms to streamline operations and remain competitive. Nepal has witnessed several significant cyberattacks that underscore the growing threat to its digital infrastructure. On June 27, 2017, the official website of the Department of Passport was infiltrated by a group of Turkish hackers. The attack resulted in the defacement of the website, accompanied by threatening notes demanding access to sensitive government data. These incident highlighted vulnerabilities in government-run digital platforms. Later that year, on October 23, 2017, NIC Asia Bank fell victim to a major breach in its SWIFT system. Unidentified hackers exploited the system to siphon off USD 4.4 million to accounts in six different countries. Although the bank managed to recover approximately USD 4 million, the incident exposed the risks associated with digital financial operations and underscored the need for robust cybersecurity measures in the banking sector. In September 2020, a cybercrime involving cloned debit cards shocked the nation. Five Chinese nationals were apprehended while attempting to withdraw cash illegally. The culprits had hacked the Nepal Electronic Payment System (NEPS), an interface facilitating inter-bank transactions, further revealing weaknesses in Nepal's electronic payment infrastructure. A more severe disruption occurred on January 27, 2023, when a Distributed-Denial-of-Service (DDoS) attack targeted Nepal's National Portal and 500 other government websites with the.gov.np domain. The Government Integrated Data Centre (GIDC)

was severely compromised, disrupting immigration and passport management systems. The attack caused operational chaos at Tribhuvan International Airport, delaying numerous international flights for hours as immigration desks failed to process travel clearances for passengers[1], [2], [3], [4], [5]. However, this rapid digitization exposes them to significant cybersecurity risks, such as ransomware, phishing, malware attacks, and data breaches. Despite their critical role in the economy, SMBs often lack the resources, expertise, and infrastructure required to defend against evolving cyber threats[6], [7], [8], [9].

Unlike large organizations, SMBs face unique challenges in cybersecurity. Limited budgets restrict investments in advanced technologies and trained personnel, while low awareness about cyber threats leads to poor implementation of security practices. In Nepal, these challenges are compounded by a lack of government support, absence of tailored security solutions, and minimal organizational preparedness[10], [11], [12], [13]. As a result, SMBs remain prime targets for cybercriminals, who exploit their vulnerabilities to gain unauthorized access to critical data and disrupt operations[14], [15].

Small and Medium Enterprises (SMEs) in Nepal are increasingly exposed to diverse cybersecurity risks due to their growing dependence on digital technologies and insufficient security frameworks. Among the most prevalent threats are phishing and social engineering attacks, where malicious actors deploy deceptive communications to extract sensitive information, including access credentials and financial data. The absence of comprehensive cybersecurity training among employees exacerbates these vulnerabilities, leaving organizations prone to exploitation. Ransomware attacks present another formidable challenge, as cybercriminals encrypt essential business data and demand payment for its restoration, often paralyzing operations. The lack of consistent data backup mechanisms further amplifies the repercussions, forcing SMEs to navigate significant operational and financial dilemmas. Malware infiltration similarly undermines business integrity, exploiting unsecured networks and obsolete systems to breach defenses. Such incursions frequently result in the theft of critical data and prolonged system downtimes. Insider threats, whether deliberate or inadvertent, also compromise organizational security[16], [17], [18], [19].

Limited monitoring and poorly defined cybersecurity protocols magnify the risks posed by internal actors, highlighting gaps in preventive measures. Furthermore, the adoption of digital payment systems by SMEs has introduced additional vulnerabilities, including exposure to fraudulent activities such as unauthorized transactions and card-skimming. The absence of robust payment security systems compounds these challenges, jeopardizing both enterprise finances and consumer trust. Weak network defenses remain a pervasive issue, characterized by unprotected wireless networks, inadequate firewalls, and unsecured endpoints. These deficiencies leave SMEs susceptible to a spectrum of cyberattacks, compromising data integrity and undermining operational reliability. Without proactive measures, such as investment in cybersecurity infrastructure, employee training, and the establishment of robust protocols, these enterprises risk severe operational disruptions and reputational harm in an increasingly digital marketplace. This study delves into the cyber defense challenges confronting SMEs in Nepal, examining their preparedness, resource limitations, and awareness levels. Employing a mixed-method research design encompassing quantitative surveys and qualitative interviews—it seeks to provide a nuanced understanding of the prevailing cybersecurity landscape. The research aims to uncover critical vulnerabilities, assess the effectiveness of current defense strategies, and propose actionable recommendations for mitigating risks while fostering resilience in the SME sector[14], [20], [21], [22], [23], [24]:

1. To identify the key cyber threats faced by SMBs.
2. To analyze the barriers to effective cybersecurity implementation.
3. To evaluate the impact of cyberattacks on SMB operations.
4. To recommend cost-effective and practical strategies for enhancing SMB cybersecurity resilience.

II. Methodology

For this research on "Cyber Defense Challenges: A Perspective from Small and Medium-Sized Businesses in Nepal," a total of **225** survey questionnaires were distributed to various small and medium-sized enterprises (SMEs) across different sectors in Nepal. The survey was designed to gather data on the cybersecurity practices, challenges, and awareness levels of these businesses.

Out of the **225** distributed surveys, **151** responses were received, resulting in a **67.1% response rate**. This response rate is considered strong and provides a solid foundation for drawing meaningful conclusions about the cybersecurity landscape among SMEs in Nepal. Additionally, a select group of **7** key individuals, including business owners and IT managers, were interviewed to gain deeper insights into specific cybersecurity issues and strategies.

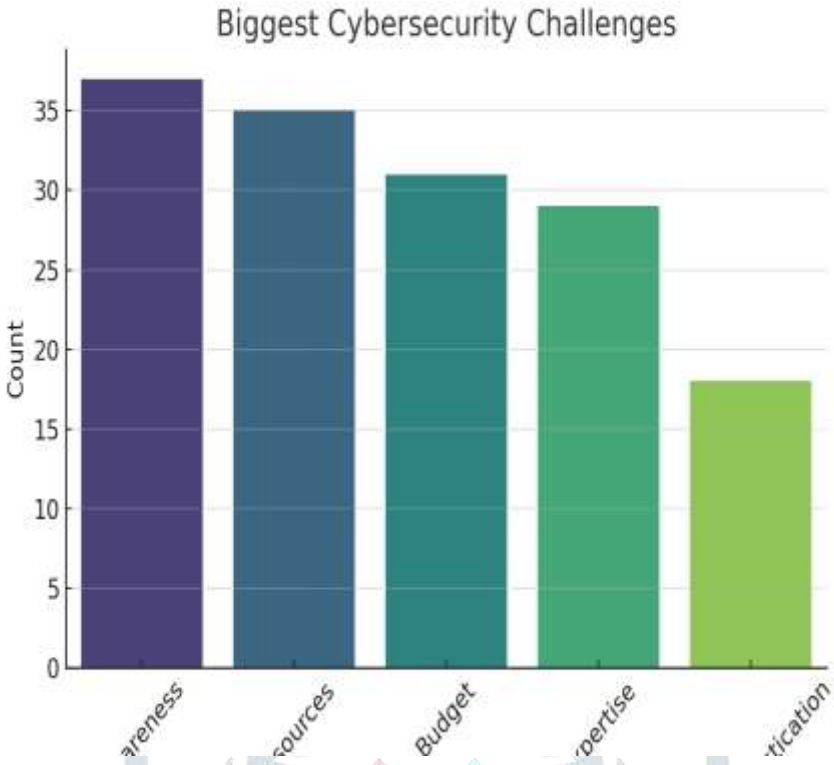
The data collected from both the survey and the interviews were analyzed to identify common trends, challenges, and gaps in cybersecurity practices among SMEs in Nepal, contributing to the development of actionable recommendations for enhancing cyber defense strategies within this sector[18], [19], [25], [26], [27].

III. Results and Discussion

1. Organization Size Distribution

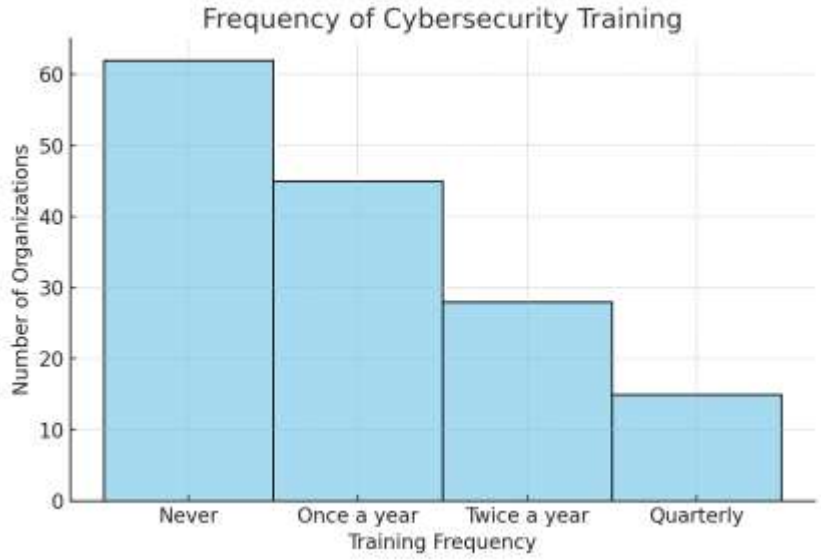
The pie chart showcasing the organization size distribution highlights that micro and small businesses dominate, each constituting 40% of the surveyed organizations, while medium-sized businesses make up the remaining 20%. This distribution underscores the critical need for cyber defense strategies to focus on micro and small businesses due to their prevalence. These smaller organizations are particularly vulnerable to cyber threats as they often lack the necessary resources, expertise, and infrastructure to implement robust cybersecurity measures. Budgetary constraints and limited technical know-how further exacerbate their susceptibility to phishing, ransomware, and malware attacks. Given their significant contribution to the local economy in terms of employment and GDP, securing this segment is essential to prevent widespread economic and social disruptions. Meanwhile, medium-sized organizations, though fewer in number, manage more complex operations and potentially sensitive data, necessitating tailored cybersecurity interventions to address their unique risks and challenges. Together, these insights point to a prioritized, resource-sensitive approach to cybersecurity for Nepal's diverse organizational landscape.

2. Biggest Cybersecurity Challenges



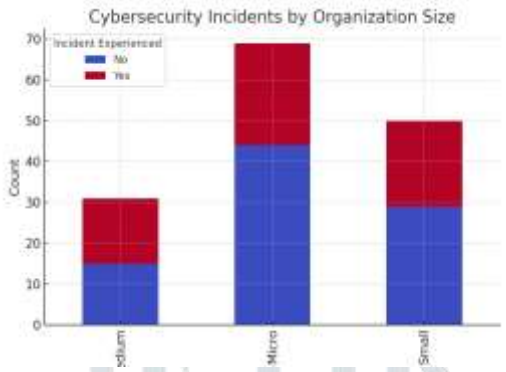
The analysis highlights the most significant challenges faced by organizations in strengthening their cybersecurity defenses. A lack of resources and expertise emerges as the most pressing issues, each cited by 25% of respondents. This indicates that organizations struggle to acquire skilled personnel and necessary tools to safeguard against cyber threats. Budget constraints and awareness issues, both accounting for 20%, further compound the problem, as limited funding restricts investments in cybersecurity solutions and low awareness hampers the adoption of best practices. Interestingly, only 10% of respondents emphasized the sophistication of cyber threats as a major concern, suggesting that many organizations may be more focused on addressing foundational challenges rather than advanced threat dynamics. To bridge these gaps, initiatives such as targeted training programs to build expertise and better resource allocation for cybersecurity infrastructure are critical. These measures can empower organizations, particularly smaller ones, to develop more resilient cyber defenses.

3. Frequency of Cybersecurity Training



The findings reveal a concerning trend regarding cybersecurity training among organizations. A significant 40% of organizations never conduct any form of training, indicating a critical gap in fostering cybersecurity awareness and preparedness. Among those that do provide training, only 10% conduct it quarterly, while others adhere to less frequent schedules, such as annual or biannual sessions. This infrequent training leaves employees and stakeholders ill-equipped to recognize and respond to emerging cyber threats, increasing the organization's vulnerability to attacks. To address this issue, it is essential to increase the frequency of cybersecurity training programs. Regular and consistent training not only enhances awareness but also helps inculcate a culture of proactive cyber hygiene, thereby reducing risks and improving overall organizational resilience.

4. Cybersecurity Incidents by Organization Size



The analysis indicates that micro and small businesses are more likely to report cybersecurity incidents compared to medium-sized organizations. Despite this, the majority of organizations across all categories reported no incidents, potentially reflecting a lack of detection capabilities or underreporting rather than an absence of attacks. Micro businesses stand out with the highest ratio of reported incidents, underscoring their heightened vulnerability. This increased susceptibility could be attributed to their limited resources, lack of dedicated cybersecurity infrastructure, and lower awareness levels. These findings highlight the need for targeted support for smaller businesses, including affordable security solutions, awareness programs, and incident response training, to help them better protect themselves and mitigate risks

5. Confidence in Prevention by Role

The findings reveal a disparity in confidence levels regarding the prevention of cyberattacks across different organizational roles. IT managers demonstrate the highest confidence, reflecting their technical expertise and familiarity with cybersecurity measures. In contrast, business owners and general employees display greater neutrality or a lack of confidence in their ability to prevent attacks. This gap suggests that non-IT staff may have limited awareness or understanding of the organization's cybersecurity practices, which could hinder collective efforts to strengthen defenses. To address this, educating non-IT staff about cybersecurity protocols and their role in mitigating risks is essential. Comprehensive training programs and awareness campaigns can empower all employees, fostering a shared sense of responsibility and boosting confidence across roles in combating cyber threats.

IV. Conclusion

The research on Cyber Defense Challenges: A Perspective from Small and Medium-Sized Businesses in Nepal has provided valuable insights into the state of cybersecurity within this sector. Based on the findings from the survey and interviews with businesses, the following conclusions can be drawn:

1. **Cybersecurity Awareness and Investment Challenges**

   Small and medium-sized businesses (SMBs) in Nepal are increasingly recognizing the importance of cybersecurity but face significant challenges in allocating sufficient resources. The limited budgetary allocations for cybersecurity often result in businesses only implementing basic protective measures, such as firewalls and antivirus software. However, more advanced technologies, such as intrusion detection systems and endpoint protection, are not widely adopted due to financial constraints. This highlights the need for more affordable cybersecurity solutions tailored to the needs of SMBs.

2. **Lack of Awareness and Understanding of National Policies**

   While some businesses are aware of national cybersecurity policies and regulations, the general awareness remains low. Many small businesses lack knowledge of the legal frameworks that could help them better protect their systems. This gap points to the need for more effective communication and education from the government regarding existing policies and their importance for businesses' security.

3. **Perceived Readiness and Confidence Levels**

   The research indicates varying levels of confidence in the ability of SMBs to prevent, detect, and respond to cyber threats. Many businesses are only moderately confident in their cybersecurity preparedness, primarily due to the lack of advanced tools and employee training. However, there is a clear recognition of the need for improvement, with many businesses indicating plans to invest in better cybersecurity practices, such as more advanced technologies and structured employee training programs. This shows a growing awareness of the need to strengthen cyber defense measures.

4. **Role of External Support and Collaboration**

   Many businesses collaborate with external cybersecurity experts for risk assessments, vulnerability testing, and the implementation of security technologies. This reliance on external expertise underscores the lack of in-house cybersecurity knowledge and resources. While some businesses are able to afford this collaboration, others struggle to access such services due to cost limitations.

5. **Government Support and Policy Recommendations**

   A key finding of this research is the widespread belief among businesses that the government could play a more proactive role in enhancing cybersecurity. Suggestions for government support include providing financial incentives, cybersecurity training programs for employees, and clearer regulatory guidelines. Businesses also emphasized the need for more affordable cybersecurity resources and greater collaboration between the government and private cybersecurity firms to strengthen the overall defense posture of SMBs.

6. **Future Steps and Improvements**

   Respondents expressed a strong interest in improving their cybersecurity capabilities in the future. Many businesses indicated that they would prioritize investments in advanced security technologies, better employee training programs, and the development of comprehensive cybersecurity policies. However, the challenge remains in finding cost-effective solutions that fit within their financial constraints. Partnerships with government agencies and external cybersecurity experts were viewed as critical steps in overcoming these barriers.

This research highlights that while small and medium-sized businesses in Nepal recognize the importance of cybersecurity, significant gaps in awareness, investment, and preparedness remain. The research underscores the need for both government and private sector collaboration to address the unique challenges faced by SMBs in the digital age. By focusing on affordable cybersecurity solutions, better training, and clearer regulations, Nepal can empower its SMBs to defend against growing cyber threats, thereby fostering a more secure and resilient digital economy.

References

[1] R. K. Shrestha, "Mapping the Entrepreneurial Ecosystem of Nepal," 2024, pp. 57–85. doi: 10.1007/978-981-97-6560-7_4.

[2] J. Bharadiya, "Machine Learning in Cybersecurity: Techniques and Challenges," *Eur. J. Technol.*, vol. 7, no. 2, pp. 1–14, Jun. 2023, doi: 10.47672/ejt.1486.

[3] M. Gupta, C. Akiri, K. Aryal, E. Parker, and L. Praharaj, "From ChatGPT to ThreatGPT: Impact of Generative AI in Cybersecurity and Privacy," *IEEE Access*, vol. 11, pp. 80218–80245, 2023, doi: 10.1109/ACCESS.2023.3300381.

[4] J. Prümmer, T. van Steen, and B. van den Berg, "A systematic review of current cybersecurity training methods," *Comput. Secur.*, vol. 136, p. 103585, Jan. 2024, doi: 10.1016/j.cose.2023.103585.

[5] R. Kaur, D. Gabrijelčič, and T. Klobučar, "Artificial intelligence for cybersecurity: Literature review and future research directions," *Inf. Fusion*, vol. 97, p. 101804, Sep. 2023, doi: 10.1016/j.inffus.2023.101804.

[6] A. Chidukwani, S. Zander, and P. Koutsakis, "A Survey on the Cyber Security of Small-to-Medium Businesses: Challenges, Research Focus and Recommendations," *IEEE Access*, vol. 10, pp. 85701–85719, 2022, doi: 10.1109/ACCESS.2022.3197899.

[7] D. Kant and A. Johannsen, "Evaluation of AI-based use cases for enhancing the cyber security defense of small and medium-sized companies (SMEs)," *Electron. Imaging*, vol. 34, no. 3, pp. 387-1-387–8, Jan. 2022, doi: 10.2352/EI.2022.34.3.MOBMU-387.

[8] H. Jahankhani, L. N. K. Meda, and M. Samadi, "Cybersecurity Challenges in Small and Medium Enterprise (SMEs)," 2022, pp. 1–19. doi: 10.1007/978-3-030-98225-6_1.

[9] A. Papathanasiou, G. Liontos, A. Katsouras, V. Liagkou, and E. Glavas, "Cybersecurity Guide for SMEs: Protecting Small and Medium-Sized Enterprises in the Digital Era," *J. Inf. Secur.*, vol. 16, no. 01, pp. 1–43, 2025, doi: 10.4236/jis.2025.161001.

[10] M. Figueredo Franco, F. Martins Lacerda, and B. Stiller, "A framework for the planning and management of cybersecurity projects in small and medium-sized enterprises," *Rev. Gestão e Proj.*, vol. 13, no. 3, pp. 10–37, Dec. 2022, doi: 10.5585/gep.v13i3.23083.

[11] A. Alahmari and B. Duncan, "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)*, IEEE, Jun. 2020, pp. 1–5. doi: 10.1109/CyberSA49311.2020.9139638.

[12] A. Cartwright, E. Cartwright, and E. S. Edun, "Cascading information on best practice: Cyber security risk management in UK micro and small businesses and the role of IT companies," *Comput. Secur.*, vol. 131, p. 103288, Aug. 2023, doi: 10.1016/j.cose.2023.103288.

[13] O. Elezaj, S. Y. Yayilgan, M. Abomhara, P. Yeng, and J. Ahmed, "Data-Driven Intrusion Detection System for Small and Medium Enterprises," in *2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)*, IEEE, Sep. 2019, pp. 1–7. doi: 10.1109/CAMAD.2019.8858166.

[14] R.-C. Härting, G.-N. Schulz, D. Deffner, and C. Karg, "Digital Transformation and Cyber Threats for Small and Medium Sized Enterprises," 2023, pp. 161–170. doi: 10.1007/978-981-99-3068-5_15.

[15] T. Tam, A. Rao, and J. Hall, "The good, the bad and the missing: A Narrative review of cyber-security implications for australian small businesses," *Comput. Secur.*, vol. 109, p. 102385, Oct. 2021, doi: 10.1016/j.cose.2021.102385.

[16] A. M. Nassef, M. A. Abdelkareem, H. M. Maghrabie, and A. Baroutaji, "Review of Metaheuristic Optimization Algorithms for Power Systems Problems," *Sustainability*, vol. 15, no. 12, p. 9434, Jun. 2023, doi: 10.3390/su15129434.

[17] L. Gupta, "Issues of Cyber security and its solutions in Nepalese Context," *NPRC J. Multidiscip. Res.*, vol. 1, no. 2, pp. 122–127, Sep. 2024, doi: 10.3126/nprcjmr.v1i2.69333.

[18] M. Garuba, C. Liu, and D. Fraites, "Intrusion Techniques: Comparative Study of Network Intrusion Detection Systems," in *Fifth International Conference on Information Technology: New Generations (itng 2008)*, IEEE, Apr. 2008, pp. 592–598. doi: 10.1109/ITNG.2008.231.

[19] S. Jagadish, S. H. Krishna, D. Sundaranarayana, H. N. Patel, M. Tiwari, and P. K. Lakineni, "Blockchain Technology to Improve Cybersecurity: Opportunities and Challenges," in *2023 Second International Conference on Informatics (ICI)*, IEEE, Nov. 2023, pp. 1–6. doi: 10.1109/ICI60088.2023.10420983.

[20] M. Kumar and H. Gupta, "A Review of Cyber Security Challenges and Mitigation Strategies in Industry 4.0 Technologies," in *2023 5th International Conference on Advances in Computing, Communication Control and Networking (ICAC3N)*, IEEE, Dec.

2023, pp. 1676–1682. doi: 10.1109/ICAC3N60023.2023.10541435.

[21] M. F. Safitra, M. Lubis, and H. Fakhrurroja, "Counterattacking Cyber Threats: A Framework for the Future of Cybersecurity," *Sustainability*, vol. 15, no. 18, p. 13369, Sep. 2023, doi: 10.3390/su151813369.

[22] S. Furnell, "Cyber Security for SMEs - Clear, Consistent and Complete?," in *European Interdisciplinary Cybersecurity Conference*, New York, NY, USA: ACM, Jun. 2024, pp. 224–224. doi: 10.1145/3655693.3661829.

[23] I. Jada and T. O. Mayayise, "The impact of artificial intelligence on organisational cyber security: An outcome of a systematic literature review," *Data Inf. Manag.*, vol. 8, no. 2, p. 100063, Jun. 2024, doi: 10.1016/j.dim.2023.100063.

[24] P. Ghimire, S. K. Piaralal, S. Raghavan, and V. S. Rethina, "Exploring Sustainability in Cloud Computing Adoption among SMEs in Nepal: A Conceptual Model," *Int. J. Acad. Res. Bus. Soc. Sci.*, vol. 14, no. 11, Nov. 2024, doi: 10.6007/IJARBSS/v14-i11/23347.

[25] S. Pokharel, "Development in Digital Capitalism: Challenges and Prospects of Nepal," *KMC Res. J.*, vol. 7, no. 1, pp. 101–111, Dec. 2023, doi: 10.3126/kmcrj.v7i1.65080.

[26] S. Latha and S. J. Prakash, "A survey on network attacks and Intrusion detection systems," in *2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS)*, IEEE, Jan. 2017, pp. 1–7. doi: 10.1109/ICACCS.2017.8014614.

[27] A. Paya, S. Arroni, V. García-Díaz, and A. Gómez, "Apollon: A robust defense system against Adversarial Machine Learning attacks in Intrusion Detection Systems," *Comput. Secur.*, vol. 136, p. 103546, Jan. 2024, doi: 10.1016/j.cose.2023.103546.

Appendix:

Section A: Demographics

1. **What is the size of your organization?**
    - Micro (1–10 employees)
    - Small (11–50 employees)
    - Medium (51–250 employees)
2. **What is your role in the organization?**
    - Owner/Executive
    - IT Manager
    - Employee
    - Other (please specify)
3. **Which industry does your business belong to?**
    - Retail
    - Manufacturing
    - IT and Software
    - Hospitality
    - Other (please specify)
4. **How long has your business been operating?**
    - Less than 1 year

- 1–5 years
- 6–10 years
- More than 10 years

Section B: Current Cybersecurity Practices

5. **Does your organization have a dedicated IT team?**
   - Yes
   - No
6. **Do you currently use any cybersecurity measures or tools?**
   - Yes
   - No
7. **If yes, what types of cybersecurity measures are in place?** (Select all that apply)
   - Firewalls
   - Antivirus software
   - Encryption
   - Multi-factor authentication (MFA)
   - Other (please specify)
8. **How often do you conduct cybersecurity training for employees?**
   - Never
   - Once a year
   - Twice a year
   - Quarterly

Section C: Cybersecurity Challenges

9. **What are the biggest cybersecurity challenges your business faces?** (Rank from 1-5, where 1 is the most critical challenge)
   - Lack of resources
   - Lack of expertise
   - Budget constraints
   - Lack of awareness among employees
   - Increasing sophistication of cyber threats

10. **Have you experienced any cybersecurity incidents in the last 12 months?**
    - Yes
    - No
11. **If yes, what type of incident occurred?** (Select all that apply)
    - Phishing attacks
    - Malware attacks
    - Data breaches
    - Ransomware
    - Other (please specify)
12. **What were the consequences of the incident(s)?** (Select all that apply)
    - Financial loss
    - Operational disruption
    - Loss of customer trust
    - Regulatory penalties
    - Other (please specify)

Section D: Perceptions and Preparedness

13. **How confident are you in your business's ability to prevent cyberattacks?**
    - Very confident
    - Somewhat confident
    - Neutral
    - Not confident
14. **How important do you think cybersecurity is for your business?**
    - Extremely important
    - Very important
    - Moderately important
    - Not important
15. **What do you believe is the primary responsibility for improving cybersecurity in your organization?**
    - Owners/Executives
    - IT Team
    - Employees
    - External consultants

Section E: Needs and Recommendations

16. **What kind of support would help your business improve its cybersecurity?** (Select all that apply)
    - Government subsidies or grants
    - Access to affordable tools
    - Free or low-cost training programs
    - Partnerships with cybersecurity firms
    - Other (please specify)
17. **Would you be willing to invest more in cybersecurity if provided with clearer benefits?**
    - Yes
    - No
18. **Do you believe the government or related institutions should take a more active role in supporting small and medium-sized businesses in Nepal to enhance cybersecurity?**
    - Strongly agree
    - Agree
    - Neutral
    - Disagree
    - Strongly disagree

Section F: Open-Ended Questions

19. **What are your biggest concerns about cybersecurity in the coming years?**
20. **What suggestions do you have for policymakers or industry leaders to help businesses like yours improve cybersecurity?**