

Cybersecurity Challenges in Nepalese SMEs: The Missing Role of Executive Leadership

Gobinda Bahadur Thapa^{1*}, Suman Thapaliya¹, and Sangita Panta¹

¹Texas College of Management & IT, Kathmandu, Nepal

*Correspondance: thapa677@gmail.com;

Keywords

Cybersecurity
Executive Leadership
Cyber Risk Management
Cybersecurity Policy
Digital Threats
Cyber Awareness

Abstract

Cybersecurity risks are becoming more significant for small and medium-sized businesses (SMEs) in today's fast-paced, digitally driven corporate climate. Examining the cybersecurity hazards encountered by small and medium-sized enterprises (SMEs) in Nepal and the part played by executive leadership in mitigating these risks is the focus of this research. Using a combination of quantitative surveys and qualitative interviews, the research examines a range of SME industries. Cyber events have affected 68% of Nepalese SMEs, according to the results; however, the majority of these businesses do not have any kind of written policy, training, or strategic supervision. Leadership is a key factor in resilience, as indicated by a somewhat favorable connection ($r = 0.52$) between executive participation and organizational cybersecurity preparation. Core hurdles to effective cybersecurity governance, according to the report, include digital threat underestimates, low cyber knowledge, and broad misunderstandings among SME leaders. Key preparedness measures reveal that Nepalese SMEs are behind their worldwide peers, according to the comparative research. To enhance cybersecurity in Nepal's SME ecosystem, the report finishes by stressing the importance of frameworks based around leadership, policy recommendations, and capacity-building programs.

Received: 5 August 2025

Revised: 2 November 2025

Accepted: 3 December 2025

ISSN: 3059 - 9687

Copyright: @Author(s) 2024

1. Introduction

Cybersecurity is now a major issue for companies all over the globe as digital transformation changes the way businesses operate. The backbone of Nepal's economy, small and medium enterprises (SMEs), is becoming more and more dependent on digital platforms for efficient communication, financial transactions, customer interaction, and operations (Madan, 2020). But these businesses are also more vulnerable to cyber dangers like phishing, malware incursions, ransomware, and data breaches because of their increasing reliance on digital technologies. Many small and medium-sized enterprises (SMEs) in Nepal do not have the means, knowledge, or plans to safeguard themselves against cyber threats, in contrast to larger companies that have established cybersecurity departments (Khadka et al., 2025).

Cybersecurity attacks in Nepal's SME sector often remain undetected until they cause extensive harm. These businesses have become easy prey for hackers due to a lack of organized cybersecurity policy, inadequate employee understanding, and inadequate investment in digital security solutions. The widespread absence of leadership buy-in and prioritized cybersecurity efforts only serves to exacerbate the situation. Most small and medium-sized enterprises (SMEs) in Nepal still view cybersecurity more as a technical issue than a strategic management concern. As a result, most companies are ill-prepared to confront the ever-changing digital threats (Cook, 2017).

Executive leadership heavily influences the tone a business sets for its cybersecurity preparedness. Their participation in activities such as risk assessment, policymaking, resource allocation, and capacity building heavily contributes to the development of a cyber-resilient corporate culture. The proactive engagement of leaders of SMEs is even more crucial in Nepal, a country with weak regulatory enforcement and low levels of digital literacy (Loonam, 2020). If they are aware of, committed to, and have a plan for it, cybersecurity can become a proactive strategic asset rather than a reactive expense.

This study takes a look at the cybersecurity issues that small and medium-sized enterprises (SMEs) in Nepal are dealing with and analyzes how senior leadership is handling these risks. This study seeks to offer practical techniques that might allow Nepalese SMEs to confidently and sustainably navigate the increasing threat landscape by studying the nexus of management involvement and cyber resilience.

1.1. Research Objectives

The primary objective of this research is to explore the cybersecurity challenges faced by Small and Medium Enterprises (SMEs) in Nepal and to critically examine the role of executive leadership in addressing these challenges. The study aims to identify gaps, opportunities, and strategic interventions that can strengthen cybersecurity resilience in Nepalese SMEs.

Specific Objectives:

1. To identify the key cybersecurity threats and vulnerabilities prevalent among SMEs in Nepal.
2. To assess the level of cybersecurity awareness, preparedness, and practices within Nepalese SMEs.
3. To evaluate the role of executive leadership in shaping cybersecurity strategies, policies, and decision-making in SMEs

2. Literature Review:

Cybersecurity is no longer considered an optional extra, largely due to the increasing number of cyberattacks on small and medium-sized businesses (SMEs). It is widely recognized that small and medium-sized enterprises (SMEs) are more vulnerable to cyberattacks than larger organizations (Truong et al., 2024). This is because SMEs often have fewer resources, fewer IT specialists, and lower levels of cybersecurity maturity (Kabanda et al., 2018). Nearly 43% of cyberattacks occur against small organizations, and most of those businesses aren't ready to respond well, says the International Telecommunication Union (2020). When digital revolution outstrips cybersecurity understanding and infrastructure development, as is happening in emerging nations like Nepal, the risk becomes much more obvious (Bruggemann et al., 2022).

Core difficulties confronting SMEs include inadequate infrastructure, lack of knowledge, and poor execution of cybersecurity policies, according to several research studies. Because of their perceived insignificance as targets, small and medium-sized enterprises (SMEs) frequently fail to adequately assess their susceptibility (Fagbule, 2023). But criminals see them as simple targets for financial extortion or points of entrance into bigger supply systems. Also, most SMEs don't conduct risk assessments often, which makes it extremely difficult for them to foresee or be ready for cyber risks (Pawar et al., 2023).

Infrastructure constraints, lax government cybersecurity regulation, and a lack of cybersecurity training programs all amplify these problems in the South Asian region and in Nepal in particular (ESCAP, 2023). According to research on small and medium-sized enterprises (SMEs) in Nepal conducted by (Maharjan & Adhikari, 2022), these organizations are particularly vulnerable to cybercrimes like phishing and ransomware because of their reliance on antiquated software, unprotected Wi-Fi networks, and lack of adequate access control measures.

Executive leadership heavily influences a company's cybersecurity posture. When cybersecurity is a top priority for leadership, it increases the likelihood that the firm will implement proactive security measures, provide awareness training, and devote enough funds to IT security (Dutta & McCrohan, 2002). According to (Von & Van, 2013), leaders that see cybersecurity as a danger to their company rather than an IT issue are more likely to cultivate a resilient culture.

Even more so in SMEs, where owners and executives frequently juggle several responsibilities and have the final say over major policy choices, leadership has a profound impact. According to (Radanliev et al., 2020), the level of commitment from leadership best predicts a small or medium-sized enterprise's (SME) capacity to identify, avoid, and deal with cyber risks. This position is especially important in developing nations without established institutions. While there is a dearth of data on the topic in Nepal, some early studies (Shrestha, 2021) indicate that cybersecurity is not a top priority for SME leaders until they are forced to do so by events outside their control, including cyberattacks or customer requests. (Ghimire et al., 2023) identify the top management's lack of digital literacy as a persistent obstacle. Only 22% of SME executives in Nepal had received cybersecurity training.

The literature often highlights the disparity between knowledge and action. Although some executives of SMEs may acknowledge the significance of cybersecurity, they frequently do not possess the necessary knowledge or resources to establish suitable safeguards (CISCO, 2021). To strengthen systemic resilience, the World Economic Forum (2022) suggests that cybersecurity should be a part of corporate governance, particularly for smaller businesses. Some have suggested that educational programs, leadership development efforts, and actions at the policy level may help. For instance, there has been encouraging evidence that government-supported cybersecurity awareness initiatives for SMEs, like the ones tested in Southeast Asia (ADB, 2020), can increase CEO engagement and readiness.

The leadership factor in particular is understudied in Nepali literature, which is surprising given the growing interest in cybersecurity for small and medium-sized enterprises (SMEs) throughout the world. Research on the effects of leadership actions, dedication, and strategic decisions on cybersecurity readiness is limited, with most research concentrating on knowledge gaps or technological deficiencies. Empirical research examining the impact of executive leadership on cybersecurity practices in small and medium-sized enterprises (SMEs) in Nepal is necessary to fill this knowledge gap.

3. Research Methodology

This study employs a mixed-methods research methodology, combining both quantitative and qualitative approaches to explore cybersecurity challenges in Nepalese SMEs and examine the role of executive leadership in addressing these threats. The research follows a descriptive and exploratory

design, enabling a broad understanding of existing cybersecurity practices while gaining deeper insights into leadership behavior and decision-making. Data will be collected through structured surveys and semi-structured interviews. The quantitative component involves a survey administered to approximately 100 SME representatives, including owners, executives, and IT personnel, focusing on cybersecurity awareness, preparedness, incident history, and leadership engagement. Purposive sampling is used to ensure participants are decision-makers or directly involved in organizational cybersecurity. The qualitative component consists of in-depth interviews with 10–15 SME executives to explore their perceptions, strategic priorities, and challenges in implementing cybersecurity measures. Quantitative data will be analyzed using descriptive and inferential statistics through SPSS, while qualitative data will undergo thematic analysis to identify recurring leadership patterns and cybersecurity gaps. Ethical considerations such as informed consent, confidentiality, and data protection are strictly maintained throughout the study. This integrated methodology provides a comprehensive understanding of how leadership impacts cybersecurity resilience in Nepal's SME sector.

4. Research Analysis

The primary goals of this study are to (1) assess the cybersecurity preparedness of small and medium-sized enterprises (SMEs) in Nepal and (2) determine the level of participation of senior leadership in the management of cyber risks. Quantitative and qualitative data are used in the study to reveal connections, trends, and areas where strategies are lacking.

4.1. Quantitative Analysis

A hundred small and medium-sized enterprises (SMEs) had their survey data evaluated using SPSS. Results showed that phishing, ransomware, and unauthorized data access were the most common types of cybersecurity incidents faced by SMEs (68%). A written cybersecurity policy was held by just 29% of the surveyed SMEs, and only 21% of those questioned performed regular risk assessments or provided training for their employees. Over 60% of people who took the survey undervalued cyber dangers, as they thought they were "not likely targets" of cyberattacks.

The association between executive engagement and organizational cybersecurity strategies was explored using a correlation study. Overall cybersecurity readiness was shown to be somewhat positively correlated with leadership engagement (as evaluated by their involvement in cybersecurity decision-making, budgeting, and training monitoring) ($r = 0.52$). Small and medium-sized enterprises (SMEs) whose leadership was actively involved were more resilient to cyber events and had preventative measures in place.

4.2. Qualitative Analysis

Twelve SME executives from the information technology (IT), retail (RET), education (ED), and hotel (HVA) industries participated in semi-structured interviews that elucidated the complex leadership perspectives on cybersecurity. The following five topics emerged from the thematic analysis of the interview transcripts:

- Most executives acknowledged having a poor technical awareness of cybersecurity and relied significantly on outside consultants or junior IT personnel, indicating a lack of cyber literacy at the leadership level.
- There was a lack of long-term strategic planning, and cybersecurity measures were often applied only after an event had occurred, rather than being proactive.
- Limited Funds: Executives frequently saw cybersecurity spending as a luxury expense, leading to a lack of funding for security software and employee education.
- IT teams were given cybersecurity duties, but they weren't closely monitored or aligned with the organization's overall objectives.
- Adaptation Intentions and Awareness on the Rise: Despite existing gaps, some leaders have shown a readiness to embrace strategy frameworks that are both accessible and inexpensive to address digital risks.

4.3. Integrated Insights

The study indicates a significant gap between the awareness of cyber dangers and the strategic responses of Nepalese SMEs' leadership, which is analyzed by integrating quantitative trends with qualitative issues. Most SMEs are still at risk due to lack of leadership and resources, despite some good practices. It is essential for SMEs to have leadership-driven cybersecurity governance due to the association between executive participation and cybersecurity preparedness.

In addition to confirming previous research on a worldwide scale, this study places that research in the context of Nepal's specific social, economic, and technical environment. To strengthen cyber resilience among Nepalese SMEs, it lays the groundwork for recommending actionable initiatives focused on leadership.

5. Results and Discussion

The results of this study show that there is a big gap between the cyber risk that small and medium-sized enterprises (SMEs) in Nepal face and the amount of preparation, knowledge, and action taken by their leadership. The majority of Nepalese SMEs still don't have any kind of written cybersecurity policy in place, much less a framework for conducting regular risk assessments, even though digital technologies are becoming more important to their daily operations. This trend is indicative of a larger pattern: cybersecurity is still seen as an ancillary technological problem, not an essential part of running a company. The study's findings showing a somewhat favorable link between executive participation and cybersecurity preparation highlight the importance of leadership in creating a safe workplace. Executives understand the importance of cybersecurity, but they are unable to make proactive decisions due to a lack of technical knowledge, financial limits, and a reactive mentality, according to interviews. The lack of accessible training programs, regulatory enforcement, and industry-specific recommendations on cybersecurity governance in Nepal further makes these difficulties worse. In spite of this, encouraging signs surfaced from the qualitative replies, suggesting that leadership is becoming more cognizant of the need for cybersecurity and that many executives are prepared to invest in the field in exchange for tangible assistance. Based on these findings, it appears that government-led efforts, awareness campaigns, and targeted leadership training might significantly enhance

cybersecurity resilience among small and medium-sized enterprises (SMEs) in Nepal. The conversation points out the desire to put senior leadership at the heart of cybersecurity strategy design and implementation and the necessity to transform our thinking from reactive defense to proactive governance.

5.1. Research Finding

Several important conclusions on the cybersecurity of Nepalese SMEs and the function of top-level management in dealing with cyber threats were drawn from the study. Nearly two-thirds of small and medium-sized enterprises (SMEs) without comprehensive cybersecurity strategies had suffered a cyber incident in the previous two years, most often caused by phishing, malware, or unauthorized access. But despite this, many SMEs weren't ready for anything, investing little in cybersecurity equipment, training staff, or incident response plans. Executives at these companies frequently had no idea what they were doing when it came to cybersecurity, the survey revealed, and they left everything to the IT department without providing any strategic direction. Nevertheless, a discernible trend emerged connecting leadership engagement to enhanced cybersecurity preparedness: small and medium-sized enterprises (SMEs) whose CEOs were actively involved in cybersecurity planning, funding, and monitoring exhibited greater resistance to assaults and were more likely to establish strong security measures. Executive interviews also showed a rising risk consciousness, but they also pointed up limitations like few resources, unclear regulations, and no individualized education plans. The results indicate that small and medium-sized enterprise (SME) leaders in Nepal are not prepared to handle cybersecurity risks adequately, even if the threat environment is growing. However, with the correct information and resources, they may make significant progress.

5.2. Comparative Analysis

This comparative analysis evaluates the cybersecurity preparedness of Nepalese SMEs relative to global standards and examines the role of executive leadership within these contexts.

5.2.1. Cybersecurity Awareness and Policy Implementation

Globally, especially in developed countries, SMEs are increasingly adopting formal cybersecurity policies and frameworks, often driven by stringent regulatory requirements such as GDPR (EU) or CCPA (USA). Studies in the EU (ENISA, 2019) show that over 50% of SMEs have established cybersecurity policies and conduct regular assessments. In contrast, this study found that only **29% of Nepalese SMEs** had any formal cybersecurity policy in place, revealing a significant gap in structured planning and governance.

5.2.2. Incident Response and Training

In many industrialized nations, SMEs conduct regular cybersecurity drills and employee training programs to mitigate human error—the most common cause of breaches. For example, SMEs in Singapore and Germany frequently collaborate with national cybersecurity centers for training and support. However, in Nepal, only **21% of SMEs** reported conducting any form of regular cybersecurity training, highlighting a lack of capacity-building efforts and a dependence on reactive approaches.

5.2.3. Leadership Engagement

Executive leadership in SMEs across the developed world is increasingly involved in cybersecurity decision-making. Leadership-driven cybersecurity strategy is often embedded into business continuity

planning and risk management processes. In this study, Nepalese SME leadership engagement was found to be low, with most leaders delegating cybersecurity responsibilities to IT teams without strategic oversight. Nevertheless, the research uncovered a **moderate positive correlation ($r = 0.52$)** between executive involvement and cybersecurity resilience, reinforcing global findings that leadership plays a decisive role in cyber preparedness.

5.2.4. Perception of Threats

One of the most notable differences is in the perception of cybersecurity threats. While SMEs in advanced economies generally acknowledge cybersecurity as a major business risk, **62% of Nepalese SME leaders** believed their businesses were unlikely targets, which is a major barrier to proactive risk mitigation. This underestimation contrasts with international trends where cybersecurity is increasingly treated as a board-level issue regardless of company size.

5.2.5. Governmental and Institutional Support

Developed countries benefit from active governmental support systems such as cybersecurity subsidies, frameworks, and awareness campaigns tailored for SMEs. In Nepal, such structured support is minimal or fragmented. Many SMEs operate without guidance or access to resources, and there is a lack of sector-specific cybersecurity policy from the government, exacerbating leadership-level inaction

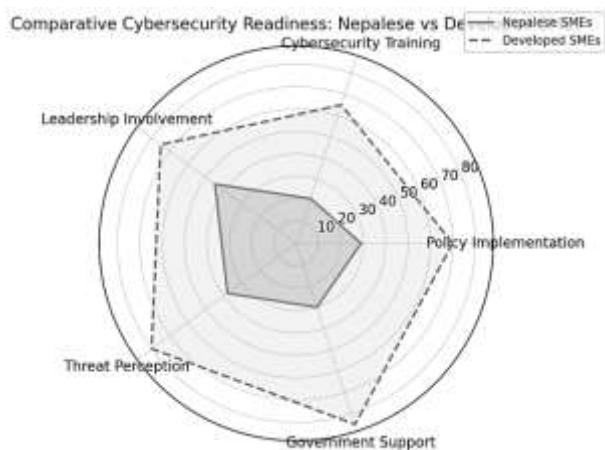


Figure 1: Comparative Cybersecurity Readiness: Nepalese Vs Developed SMEs

This illustrated comparative analysis figure shows the cybersecurity readiness of Nepalese SMEs versus developed-country SMEs across five key dimensions.

Summary of Comparative Analysis

The comparative analysis clearly shows that Nepalese SMEs lag significantly behind their global counterparts in cybersecurity readiness, largely due to limited executive engagement, poor perception of cyber threats, and lack of structural support. While technical vulnerabilities are evident, the deeper issue lies in strategic neglect—an area where executive leadership can make a transformative difference. Closing this gap will require a multi-pronged approach involving awareness, leadership training, policy support, and affordable access to cybersecurity solutions tailored for the SME ecosystem in Nepal.

5.3. Finding

The study yielded several key findings that highlight both the vulnerabilities and opportunities within Nepal's SME cybersecurity landscape. Firstly, a significant 68% of SMEs reported experiencing at least one cyber incident, with phishing and malware attacks being the most prevalent. Despite this high exposure to threats, only 29% had formal cybersecurity policies, and a mere 21% conducted regular training or awareness programs, indicating a reactive and underprepared cybersecurity posture.

A substantial 62% of SME leaders believed their organizations were unlikely to be targeted, revealing a critical misconception that smaller businesses are immune to cyber threats. This perception has contributed to low investment in cybersecurity infrastructure and personnel.

The research also found a moderate positive correlation ($r = 0.52$) between executive leadership involvement and organizational cybersecurity readiness. SMEs with proactive leadership—those who engaged in risk assessment, budgeting, and monitoring—demonstrated significantly higher levels of preparedness and resilience.

Qualitative insights revealed that many executives lacked technical knowledge and treated cybersecurity as a secondary concern until incidents forced action. However, there was a growing recognition among leaders of the importance of cybersecurity, paired with a willingness to improve if guided by accessible frameworks and resources.

In summary, the findings show that while Nepalese SMEs face considerable cybersecurity challenges, leadership plays a decisive role in shaping their digital resilience. Addressing knowledge gaps and supporting executive-level engagement will be essential for building more secure and sustainable SME ecosystems in Nepal.

5.4. Results

The results of the study provide a comprehensive view of the cybersecurity challenges faced by SMEs in Nepal and the pivotal role of executive leadership in mitigating these risks. Out of the 100 surveyed SMEs, 68% reported experiencing at least one form of cyberattack, with phishing (42%), malware (28%), and ransomware (18%) being the most common. Despite this, only 29% had implemented a formal cybersecurity policy, and 21% conducted regular cybersecurity training for employees. Furthermore, 62% of respondents believed their business was too small to be targeted, reflecting a widespread underestimation of cyber threats.

Quantitative analysis revealed a moderate positive correlation ($r = 0.52$) between leadership involvement in cybersecurity and the organization's overall security preparedness. SMEs with active executive participation in cybersecurity strategy, budgeting, and training were significantly more likely to adopt preventive measures such as firewalls, encryption, and access control systems.

Qualitative interviews with 12 SME executives revealed five recurring themes: (1) limited cyber literacy among top management; (2) a reactive approach to cybersecurity; (3) budgetary and resource constraints; (4) over-reliance on IT staff without executive oversight; and (5) a growing recognition of cybersecurity's importance. Many leaders admitted taking cybersecurity seriously only after experiencing a breach, and although awareness is increasing, practical knowledge and strategic integration remain weak.

These results underscore a critical need for leadership-focused interventions in Nepalese SMEs, including targeted training, government support, and industry-specific cybersecurity frameworks to enhance resilience and risk management capabilities.



Figure 2: representing the key research results related to cybersecurity in Nepalese SMEs

This bar chart visualizing the key research results on cybersecurity in Nepalese SMEs, including types of attacks, policy adoption, training practices, and leadership engagement.

6. Future work

This research discusses the impact of executive leadership on cybersecurity issues encountered by small and medium-sized enterprises (SMEs) in Nepal; however, there are still many unanswered questions. To start with, to make the results more applicable to a wider range of businesses and areas in Nepal, future research should extend the sample size. With the proliferation of complex digital threats, it is crucial to conduct longitudinal studies to track the changes in leadership involvement with cybersecurity.

The creation and evaluation of a leadership-centric cybersecurity framework adapted to small and medium-sized enterprises (SMEs) in developing nations such as Nepal is another encouraging avenue to pursue. Practical tools, policy templates, and risk assessment models that non-technical executives can easily adopt and administer may be included in such a framework. Research in the future may also look at how regulatory interventions, such as incentive-based compliance programs or mandated cybersecurity assessments, affect the actions and investments of SMEs. Future studies may also look at how small and medium-sized enterprises (SMEs) in Nepal might make use of affordable AI-based solutions to better identify and avoid cyberattacks, which is important because AI and automation are becoming more important in cybersecurity. Lastly, joint research involving academics, business groups, and government agencies could greatly enhance national cybersecurity capacity-building initiatives targeting SME leaders. Future study in this area can help strengthen Nepal's small and medium-sized enterprise (SME) sector's ability to withstand cyberattacks by ensuring that top executives take an active and knowledgeable role in governing digital risk.

7. Conclusion

This study evaluated the function of top-level management in handling digital dangers and investigated the cybersecurity issues encountered by Nepalese SMEs. There is a worrying disparity between the cybersecurity preparedness of Nepalese SMEs and their growing dependence on digital technology, according to the survey. Only 29% of the businesses polled had official cybersecurity policies, and just 21% provided regular training, although 68% of those businesses had encountered cyber events, including phishing, malware, and ransomware. According to these results, cybersecurity is typically seen as a reactive issue, with measures being implemented only after a breach has happened. Executive participation and overall cybersecurity preparation were shown to have a modest positive connection ($r = 0.52$), highlighting the significant role that leadership plays in building resilience. Interviews with SME executives highlighted limited cyber knowledge, low digital security priority, and the general opinion (shared by 62% of respondents) that SMEs are unlikely targets. The cybersecurity industry as a whole suffers from a poor culture, which is attributed to this belief, along with limited resources and a lack of official support.

Despite advancements in the field, cybersecurity is still primarily considered an IT department's responsibility, rather than a strategic one, according to the study talks. But small and medium-sized enterprises (SMEs) whose leadership was actively involved took a more methodical approach, carrying out tasks including risk assessment, allocating funds, and raising awareness. These examples demonstrate how effective leadership can transform cybersecurity from a liability to a competitive advantage.

When compared to their international competitors, Nepalese SMEs fall short in several areas, including training, institutional support, policy execution, and threat perception. The need for leadership-driven action is heightened in Nepalese SMEs due to the absence of government-led programs and industry frameworks that strengthen cyber resilience in industrialized nations.

To sum up, our study proves that among the many underappreciated factors in enhancing cybersecurity in Nepalese SMEs, CEO leadership is crucial. It is critical to elevate cybersecurity to the level of a strategic priority for executives to close the readiness gap. Collaborative public-private efforts focused on capacity training, streamlined policy toolkits, and leadership awareness programs can accomplish this. The ability of small and medium-sized enterprises (SMEs) in Nepal to withstand the ever-changing digital threat landscape will rely on the leadership's strategic vision and dedication as much as it does on technology.

References

- Asian Development Bank (ADB). (2020). Cybersecurity in SMEs: Case Studies from Southeast Asia. Retrieved from <https://www.adb.org>
- Bruggemann, R., Koppatz, P., Scholl, M., & Schuktomow, R. (2022). Global cybersecurity index (GCI) and the role of its 5 pillars. *Social Indicators Research*, 159(1), 125-143.
- Cisco Systems. (2021). Cybersecurity for Small and Medium-Sized Businesses: Threats and Recommendations. Retrieved from <https://www.cisco.com>
- Cook, K. D. (2017). Effective cyber security strategies for small businesses (Doctoral dissertation, Walden University).

- Dutta, A., & McCrohan, K. (2002). Management's role in information security in a cyber economy. *California Management Review*, 45(1), 67-87.
- ESCAP, U. (2023). Asia-Pacific Trade and Investment Report 2023/24: unleashing digital trade and investment for sustainable development.
- Fagbule, O. (2023). Cyber security training in small to medium-sized enterprises (SMEs): Exploring organisation culture and employee training needs (Doctoral dissertation, Bournemouth University).
- Ghimire, A., Sharma, B., & Karki, R. (2023). Cybersecurity awareness in SMEs in Nepal: A survey-based study. *Journal of ICT and Management*, 7(1), 45–59.
- Kabanda, S., Tanner, M., & Kent, C. (2018). Exploring SME cybersecurity practices in developing countries. *Journal of organizational computing and electronic commerce*, 28(3), 269-282.
- Khadka, A. K., Kaspal, A., & Khadka, S. (2025). Assessing the Contributing Factors for the Success of Small and Medium-Sized Businesses in Nepal.
- Loonam, J., Zwiigelaar, J., Kumar, V., & Booth, C. (2020). Cyber-resiliency for digital enterprises: a strategic leadership perspective. *IEEE Transactions on Engineering Management*, 69(6), 3757-3770.
- Madan, N. (2020). A review of access to finance by micro, small and medium enterprises and digital financial services in selected Asia-Pacific least developed countries.
- Maharjan, P., & Adhikari, S. (2022). Cybersecurity readiness of SMEs in Nepal. *Journal of Business and Technology*, 9(2), 31–41.
- Pawar, S. A., & Palivela, H. (2023). Importance of least cybersecurity controls for small and medium enterprises (SMEs) for better global digitalised economy. In *Smart Analytics, Artificial Intelligence and Sustainable Performance Management in a Global Digitalised Economy* (pp. 21-53). Emerald Publishing Limited.
- Radanliev, P., De Roure, D., & Walton, R. (2020). Cyber risk management in SMEs: A holistic framework. *Technological Forecasting and Social Change*, 150, 119740. <https://doi.org/10.1016/j.techfore.2019.119740>
- Shrestha, R. (2021). Executive perception and cyber risk in Nepalese SMEs. *Nepal Management Review*, 13(1), 55–70.
- Truong, T. C., & Nguyen, H. K. (2024, May). Cybersecurity in small and medium-sized enterprises: A Bibliometric analysis. In *International conference on From Smart City to Smart Factory for Sustainable Future* (pp. 392-402). Cham: Springer Nature Switzerland.
- Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *computers & security*, 38, 97-102.
- World Economic Forum. (2022). Principles for Board Governance of Cyber Risk. Retrieved from <https://www.weforum.org>