International Journal of Multidisciplinary and Innovative Research

ISSN(print): 3050-6883, ISSN(online): 3050-6891

Volume 02 Issue 06 June 2025

DOI: 10.58806/ijmir.2025.v2i6n05

Page No: 191-200

Cybersecurity Challenges in Small and Medium Enterprises (SMES) in Nepal

Gobinda Bahadur Thapa[1], Dr. Suman Thapaliya[2]

[1,2] Texas International College, Nepal

ABSTRACT

Small and Medium Enterprises (SMEs) are vital to the global economy and play a significant role in Nepal's economic growth. However, SMEs in Nepal face critical cybersecurity challenges due to limited financial resources, insufficient skilled personnel, and low awareness of cyber risks. As a result, they remain highly vulnerable to threats such as phishing, malware, and ransomware. This study surveyed SME owners and employees in Nepal to investigate their cybersecurity practices and experiences. The results reveal that many SMEs rely on outdated technology, lack formal security policies, and provide minimal cybersecurity training to staff. Consequently, these businesses are frequently at risk of cyberattacks, which can lead to severe financial losses and even business closure. To address this gap, the paper proposes an *E3-NSME* cybersecurity protocol (Easy, Economic, Efficient) – a set of straightforward, cost-effective, and efficient measures tailored for resource-constrained SMEs. Recommended steps include basic cyber hygiene practices, affordable security tools, regular training, and leveraging government support. The findings aim to guide Nepali SMEs and policymakers in strengthening cyber resilience, thereby helping secure the nation's SME sector in the digital era.

ARTICLE DETAILS

Published On:
30 June 2025

Available on:
https://ijmir.com

1 INTRODUCTION

In Nepal, SMEs are officially defined by the value of fixed assets (up to NPR 150 million) and constitute the backbone of the national economy [6]. Over 95% of business enterprises in Nepal are micro, small, or medium-sized [15], together contributing an estimated 22% of Nepal's GDP and providing about 1.7 million jobs [20]. Rapid digitalization of business processes in recent years has offered new opportunities for growth but also introduced significant cyber risks. Many Nepali SMEs are undergoing digital transformation in finance, operations, and service delivery [1]. This "digital shift" brings efficiency benefits yet exposes SMEs to cyber threats for which they are often ill-prepared [21]. Cyber incidents have already led to substantial financial losses and even business closures among SMEs globally [22, 18].

Globally, cyberattacks targeting SMEs are on the rise. Over 43% of all cyber-attacks worldwide are aimed at small businesses, yet only 14% of such businesses feel adequately prepared to defend against them [22, 7]. In the UK, for example, SMEs face an estimated 10,000 cyberattacks daily [12]. Verizon's breach analysis reported that 58% of data breach victims in 2019 were small businesses [23]. Surveys consistently show that many SMEs underestimate their risk exposure – often under the false assumption that attackers only target large corporations [2]. This complacency leads to underinvestment in security measures and training [2]. In reality, threats such as phishing, ransomware, and insider misuse can cause devastating financial and reputational damage to SMEs [9]. A European study found that 90% of SMEs would suffer serious impacts within a week of a cyber incident, and 57% might go out of business as a result [7, 8]. SMEs in developing countries are particularly vulnerable due to limited resources and cybersecurity awareness [11, 19].

Nepal is no exception. While the Government of Nepal introduced a National Cybersecurity Policy in 2016 to raise awareness and bolster cyber defenses [13, 17], most efforts have focused on critical infrastructure and larger organizations. The central bank (Nepal Rastra Bank, NRB) recently mandated stronger cyber controls for financial institutions – such as compulsory incident reporting within 24 hours and dedicated cybersecurity budgets [16] – underscoring growing concern even in regulated sectors. Yet outside the banking sector, Nepali SMEs generally lack formal guidance or regulatory requirements on cybersecurity. They often operate with constrained budgets and minimal IT expertise, making it challenging to implement advanced security controls [10]. This environment leaves a significant portion of Nepal's economy exposed to cyber risks that could undermine business continuity and growth.

Research Objective: In light of these challenges, this study aims to investigate the prevailing cybersecurity issues faced by SMEs in Nepal and to provide viable solutions and strategies for mitigating risks. The goal is to strengthen the cybersecurity resilience of Nepali SMEs amid a rapidly evolving digital environment. Specifically, the research examines how scarce resources, limited expertise, and low awareness impact the security posture of SMEs. Common vulnerabilities (e.g., lack of security policies, legacy systems, risks from cloud adoption and remote work) are analysed. The study further proposes cost-effective and feasible cybersecurity solutions tailored to
SMEs in Nepal to enhance their security posture and reduce the likelihood of cyberattacks.

Research Questions: This study is guided by several key questions:

1. How do SMEs in Nepal identify and respond to the most common types of cyber threats and attacks?
2. How effective are the cybersecurity measures and tools currently used by SMEs in Nepal?
3. What financial, technological, and awareness barriers impact the adoption of sound cybersecurity practices among Nepali SMEs?
4. What types of assistance or policies would most help SMEs bolster their cybersecurity defenses?
5. What are the main internal roles and responsibilities within SMEs for managing cybersecurity?

2 LITERATURE REVIEW

Cybersecurity has become a top priority for organizations of all sizes, yet SMEs face unique challenges due to limited resources, technical capacity, and awareness [3]. Unlike large firms, SMEs often lack dedicated IT departments and well-defined cybersecurity strategies, making them “easy targets” for cyber criminals [10, 7]. Research consistently shows that SMEs are disproportionately impacted by cyberattacks, with phishing, ransomware, and insider threats among the leading causes of financial loss and reputational damage [7]. A systematic review by [3] found pervasive gaps in cybersecurity awareness training for SMEs, indicating that traditional awareness programs have not fully bridged the knowledge deficit.

Many SME owners mistakenly believe their smaller size affords them security through obscurity. [2] noted that a majority of SMEs assume they are less likely targets, an incorrect belief that leads to underinvestment in cybersecurity infrastructure and employee training. [9] further confirmed that employees in SMEs often lack formal cybersecurity education; this makes social engineering attacks (like phishing emails) more likely to succeed [9, 7]. The human factor is indeed critical – an ENISA report highlighted that 77% of company data breaches involve internal weaknesses or insider actions (whether malicious or inadvertent) [7]. Thus, cultivating a security-aware culture in SMEs is as important as technical defenses.

The rapid adoption of new digital technologies by SMEs has expanded their threat surface. For instance, the move to cloud computing and virtual collaboration can introduce misconfiguration risks, weak access controls, and data exposure if not managed properly [21]. The COVID-19 pandemic forced many SMEs to hastily adopt remote work and online services, often without adequate security planning, which amplified vulnerabilities [18]. In developing country contexts, additional challenges come into play. [11] found that SME cybersecurity practices in South Africa were constrained by internal factors such as budget limitations, lack of top-management support, and complacent attitudes toward security [11, 19]. External pressures (e.g., client security requirements or regulatory standards) were not strongly felt by those SMEs, resulting in a lower impetus to improve security practices [11]. This suggests that without outside incentives or awareness, many SMEs tend to under-prioritize cybersecurity until after a major incident occurs.

At the same time, studies indicate that affordable best-practice measures can significantly improve SME security if adopted. For example, basic cyber hygiene steps (regular software updates, strong password policies, data backups, antivirus use, etc.) are known to prevent the majority of common attacks [4, 5]. ENISA (2020) and other agencies have published SME-focused guidelines emphasizing these fundamentals along with risk assessment and incident response planning [7, 14]. [8] highlight a range of practical solutions for SMEs – from employee awareness programs to leveraging managed security services – that can be tailored to constrained budgets. However, even when such guidance is available, the translation into practice has been slow. A recent systematic review by [19] concluded that research on SME cybersecurity remains shallow, with many studies reiterating known problems without delivering implementable solutions. They argue that limited cybersecurity literacy among SME owners is a root cause that manifests as low risk awareness and insufficient resource allocation, especially in developing regions [19, 3].

In summary, the literature underscores a clear need for targeted, affordable, and scalable cybersecurity approaches aligned with SMEs’ operational and financial constraints [7, 8]. Addressing SME cybersecurity challenges requires not only technical controls but also improvements in awareness, skills training, and supportive governance frameworks. This study builds on these insights to assess the situation in Nepal and to propose a pragmatic protocol (E3-NSME) that addresses the identified gaps in a manner feasible for SMEs.

3 METHODOLOGY

3.1 Research Design

This research employed a descriptive and exploratory survey design to collect quantitative data on cybersecurity challenges faced by SMEs in Nepal. The approach was chosen to systematically measure current awareness levels, practices, and difficulties that SMEs encounter in managing cybersecurity risks.

3.2 Sample and Sampling

The target population for the survey was SME stakeholders in Nepal with knowledge of their organization's cybersecurity (including owners, managers, IT staff, or other employees handling IT tasks). A purposive sampling strategy was used to select SMEs that actively use digital systems or internet services in their operations. Recruitment leveraged professional networks and referrals (snowball sampling), wherein initial respondents recommended other SME participants. In total,
$N = 50$ SMEs participated, spanning various sectors such as retail, services, manufacturing, and IT. The sample covered micro enterprises (under 10 employees) up to medium-sized firms (up to 250 employees), reflecting the diversity of Nepal's SME sector.

3.3 Data Collection Instrument

Data were collected via a structured questionnaire administered online (using Google Forms) and via email. The questionnaire comprised 20 statements and questions on a 5-point Likert scale (from "Strongly Disagree" to "Strongly Agree"), covering key topics: - cybersecurity knowledge and awareness, - current security practices and tools in use, - existence of policies or guidelines, employee training efforts, - resource limitations (budget, personnel), - technical measures implemented (e.g., firewalls, backups), and - use of external support or consulting.
Additionally, a few open-ended questions invited respondents to describe any recent cyber incidents and suggest what support they need most for cybersecurity. Basic demographic information about each business (size, sector, presence of IT staff) was also gathered for context.

3.4 Procedure and Ethics

Participants were invited via email and provided informed consent before taking the survey. Participation was voluntary and responses were collected anonymously. Respondents were assured that all data would remain confidential and used only for research purposes. No personally identifiable information was collected, and organizations are not named in the study. The survey was conducted in October 2024 over a four-week period.

3.5 Data Analysis

Quantitative survey data were analysed using descriptive statistics to identify trends in SME cybersecurity practices and perceptions. We calculated frequencies, percentages, and mean Likert scores for each survey item to gauge overall awareness and preparedness levels. Key results are presented in tables and charts for clarity. Where sample size allowed, we performed cross-tabulation to explore relationships between variables – for example, comparing security practices between smaller (micro) and larger (medium) SMEs, or between those with and without dedicated IT staff. However, given the modest sample size, these analyses are interpreted qualitatively.

Qualitative feedback from open-ended questions was reviewed to extract common themes regarding challenges and desired support. This helped contextualize the numerical findings and informed the development of our recommended protocol. Triangulating the quantitative and qualitative data enabled a richer understanding of the gaps in SME cybersecurity readiness.

4 RESULTS AND ANALYSIS

4.1 Profile of Respondent SMEs

The surveyed SMEs ranged from microenterprises with under 10 employees (40% of sample) to medium firms with over 100 employees (15% of sample), with the remainder falling in the small category (10–50 employees). Business sectors included retail (30%), hospitality (20%), IT services (15%), manufacturing (10%), and others (25%). About one-third (32%) of responding companies reported having at least one full-time IT or cybersecurity staff member, whereas the majority relied on non-specialist staff or external IT support for their technology needs. This variation in size and IT staffing provides context for their cybersecurity capabilities. Most businesses indicated they use computers and internet connectivity for operations (email, accounting, e-commerce, etc.), underscoring their exposure to cyber risks.

4.2 Cybersecurity Knowledge and Practices

Overall awareness of cybersecurity varied widely. Approximately 60% of respondents agreed that they are aware of common cyber threats (such as computer viruses or phishing scams), though fewer (only 30%) felt "very confident" in their knowledge. In terms of concrete practices, many SMEs have implemented basic protections: for example, about 80% reported using antivirus or anti-malware software on their systems, and 70% said they keep their operating systems and software updated at least semi-regularly. Basic network defenses like Wi-Fi passwords and router firewalls were also common. However, more advanced or policy-driven

practices were lacking. Fewer than 20% of SMEs had a written cybersecurity policy or incident response plan. Only 25% had ever conducted a vulnerability assessment or penetration test on their systems. Formal employee cybersecurity training was reported by just 15% of respondents – meaning the vast majority of SMEs do not systematically educate their staff about cyber hygiene or how to handle suspicious
incidents.

To put these findings in perspective, we compare them with trends observed in other contexts.

Figure 1 illustrates the adoption rates of various cybersecurity measures among SMEs in a recent UK survey [12]. The pattern is similar: essential tools like antivirus and software updates are relatively well-adopted, whereas measures such as multi-factor authentication and staff training lag behind. This alignment suggests that Nepali SMEs share many of the same practice gaps identified in developed countries, albeit potentially to an even greater extent.

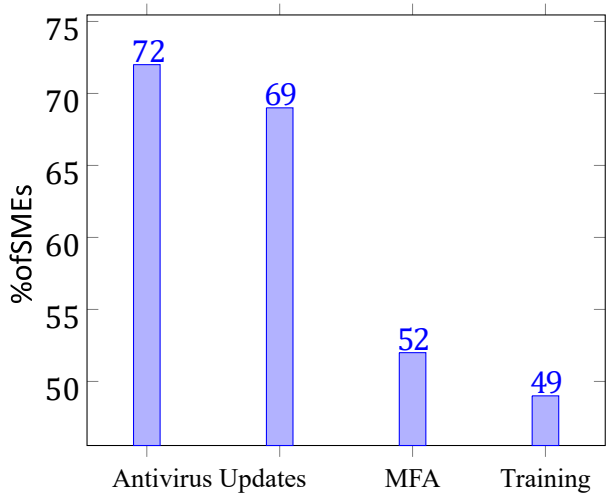

Figure 1: Adoption of cybersecurity measures among SMEs (Markel Direct UK Survey, 2024) [12].

Notably, our survey found that SMEs with any dedicated IT personnel were more likely to implement a broader range of security measures. For instance, among firms with an IT specialist, 90% used antivirus and 50% had enabled multi-factor authentication, compared to 75% and 20% respectively among firms without IT staff. This trend highlights the importance of technical expertise in driving cybersecurity uptake.

4.3 Major Threats and Incident Experience

When asked about perceived threats, respondents most frequently cited malware (viruses and worms) and phishing as the top concerns. Over half (55%) of SMEs rated phishing emails or fraudulent links as a "high" risk to their business. Similarly, 50% flagged malware infections (including ransomware) as a major worry. Fewer respondents were aware of more subtle threats like insider misuse or data leakage, although a significant portion acknowledged the general risk of employee mistakes (for example, one respondent noted: "we worry an employee could accidentally expose data or click something harmful").

In terms of actual incidents, 20% of the SMEs admitted they had experienced some form of cyber incident in the past year. The most common incidents reported were malware infections (such as computer viruses causing system outages) and phishing attacks targeting staff (e.g., fraudulent emails attempting to steal passwords or deliver malicious links). A couple of businesses described ransomware attacks in which their data was encrypted – in one case, a manufacturing company suffered two days of downtime and a financial loss of over NPR 500,000 due to a ransomware incident that halted operations. Fortunately, none of the surveyed SMEs reported permanent loss of critical data, thanks in part to ad-hoc backup practices (some mentioned saving files to external drives or cloud storage, albeit irregularly).

One troubling finding is that most incidents went unreported to authorities; SMEs generally handled them internally or simply removed the malware and moved on. This underreporting is consistent with global observations that SME breaches are often kept private [7]. It suggests that official figures may underestimate the scale of the problem in Nepal.

Table 1 summarizes prevalent cyber threats to SMEs as identified in our study and supported by international data. It highlights phishing/social engineering, malware (including ransomware), and insider-related risks as dominant categories.

4.4 Key Obstacles and Gaps

The survey asked SMEs to identify their biggest obstacles in improving cybersecurity. The responses reinforced many issues highlighted in the literature. Limited financial resources was the most common challenge – about 68% of respondents agreed that budget constraints prevented them from investing more in security tools or personnel. One respondent wrote, "We know we should do more, but cybersecurity products and experts are expensive, and we have other priorities." The next major challenge was lack of in-house expertise (cited by 54%): most SMEs do not have cy

Table 1: Common Cyber Threats to SMEs and Their Prevalence

Threat Category	Prevalence and Impact
Phishing & Social Engineering	The most frequently observed attack vector. Around 30% of small businesses worldwide consider phishing their biggest cyber threat [22]. Phishing emails are often the entry point for further attacks. Over 85% of breaches involve a human element (e.g., falling for scams) [23].
Malware (Viruses, Trojans)	A major threat accounting for roughly one-third of cyberattacks. ENISA (2020) reported malware comprises about 30% of incidents [7]. It can disrupt systems or steal data. Basic antivirus can catch known malware, but new variants still regularly evade defenses.
Ransomware	A specific subset of malware that encrypts data for ransom. It has surged in recent years, making up roughly 28% of reported attacks [22]. Even a single ransomware incident can cripple an SME's operations and lead to substantial financial losses.
Insider Threats	Security breaches caused or facilitated by internal actors (employees or contractors), whether through negligence or malicious intent. Studies find that up to 77% of data breaches in firms could involve insider actions or errors [7]. SMEs often underestimate this risk; lack of staff training and oversight exacerbates it.

bersecurity specialists and find it difficult to implement complex security measures correctly. Low awareness or perceived importance of cybersecurity among management was another theme, noted by around 50% of respondents. Some owners or managers only realized the importance of security after experiencing an incident.

Additionally, operational issues such as using outdated systems were evident. Nearly 40% admitted they still run older software (e.g., Windows 7 or older) due to cost or compatibility reasons, even though this increases vulnerability to known exploits. Around 30% mentioned difficulties in finding trustworthy external security services or knowing where to get help.

Notably, 69% of surveyed SMEs do not have any formal cybersecurity policy or guidelines (this mirrors the UK study where 69% of SMEs lacked a policy) [12]. And nearly half (48%) said they would not know the proper steps to take if a serious cyberattack occurred, beyond basic IT troubleshooting. This readiness gap underscores the need for clearer incident response planning and training.

4.5 Need for Support and Training

When asked what would most help them improve cybersecurity, respondents overwhelmingly pointed to a desire for external guidance and training. Over 80% welcomed the idea of affordable training workshops or awareness programs targeted at SME owners and staff. Many suggested that the government or industry associations could provide free or subsidized seminars, online tutorials in the Nepali language, or printed guidelines specifically designed for small businesses. Approximately 60% indicated that they would participate in cybersecurity programs if offered through a government initiative (for example, a few were aware of the Nepal Telecommunication Authority's past awareness campaigns and viewed them positively).

About half the respondents (50%) also expressed interest in having access to cybersecurity experts on an as-needed basis – for instance, a helpline or consultancy that SMEs could reach out to for advice or incident response support. This resonates with practices in other countries; in the UK, some insurance providers now include a cyber incident helpline for SME clients [12]. In Nepal, such services are not yet common, but the demand seems to be there.

Finally, many participants believe there is a role for government policy in bolstering SME cybersecurity. Suggestions included tax incentives for investing in security tools, grants or loans to upgrade legacy systems, and more stringent regulations for sectors handling sensitive data. A few respondents from the financial services sector noted that NRB's IT guidelines forced them to improve security (e.g., implementing multi-factor authentication) [16]; they suggested similar guidelines could be extended to larger SMEs or other industries in the future.

4.6 Summary of Findings

In summary, the data paint a picture of Nepal's SMEs being aware of cybersecurity in principle but underprepared in practice. Basic cyber hygiene measures are somewhat in place, but critical gaps remain in advanced protections, formal planning, and especially training. The lack of financial and human resources is a primary barrier, compounded by a tendency to delay action until after an incident occurs. These findings align with global patterns – SMEs worldwide struggle with similar issues – but the constraints appear more acute in developing economies like Nepal's. Encouragingly, SMEs are open to improvement and external support, indicating that well-crafted interventions (whether from government, industry, or academia) could significantly elevate the cybersecurity posture of this sector.

The insights from this survey directly inform the development of the E3-NSME Protocol described in the next section. This protocol is designed to address the identified gaps by providing SMEs with a clear, actionable roadmap to improve cybersecurity in a manner that is easy, costeffective, and efficient given their limitations.

5 E3-NSME CYBERSECURITY PROTOCOL FOR SMES

Based on the challenges identified, we propose a three-pronged cybersecurity protocol tailored for SMEs, named E3-NSME – emphasizing solutions that are Easy, Economic, and Efficient for small businesses to implement. This protocol is intended as a practical toolkit that SME owners and managers can follow to progressively enhance their cyber resilience without requiring extensive expertise or prohibitive investment. The key components of E3-NSME are outlined below:

- Easy – Simplify Cybersecurity: Focus on basic measures that are straightforward to adopt and do not require specialized IT skills.

- *Strong Authentication:* Enforce the use of strong passwords or passphrases for all user accounts and change default passwords on devices. Whenever possible, enable two-factor or multi-factor authentication (e.g., SMS or authenticator app verification) on email, banking, and other critical accounts [14].
- *Regular Updates and Patching:* Keep all software up to date. Activate automatic updates for operating systems, antivirus programs, web browsers, and other key applications so that known security vulnerabilities are patched promptly.
- *Baseline Protections:* Install reputable anti-malware software on all computers and ensure it is configured to scan regularly. Use the built-in firewalls on routers and PCs to block unsolicited inbound connections. These basic tools are often low-cost or free and provide
  essential first-line defense.
- *Data Backups:* Regularly back up important business data to an external hard drive or secure cloud storage. Schedule backups at least weekly (or more frequently for critical data). Test restoring from backups occasionally to ensure data integrity. In case of ransomware or data loss, having recent backups can save the business [7].
- *Employee Awareness Basics:* Provide simple do's and don'ts to all employees. For example, instruct staff to be cautious of unexpected emails or links (to counter phishing), not to plug in unknown USB drives, and to report any suspicious computer behavior. Even a brief orientation or a one-page guideline can dramatically reduce human error incidents.

- Economic – Cost-Effective Solutions: Prioritize cybersecurity steps that offer high impact for low cost, fitting within SMEs' limited budgets.

- *Leverage Free Resources:* Take advantage of free cybersecurity tools and services. For example, use free editions of cloud security services, freeware encryption tools for protecting sensitive files, and free security assessment tools (some organizations and universities offer free web vulnerability scans or risk assessment checklists for SMEs).
- *Open-Source and Cloud Services:* Consider open-source software alternatives for security (which avoid licensing costs) and utilize cloud services that have security built-in. Many cloud providers offer small businesses free tiers for services like secure email, file storage with encryption, and basic website security features.
- *Budget for Essentials:* Allocate a modest annual budget specifically for cybersecurity needs. Even 5–10% of the IT budget earmarked for security can cover essentials like an upgraded antivirus suite, a secure Wi-Fi router, or an hour of professional consultation. Notably, NRB now requires financial institutions to dedicate part of their budget to cybersecurity [16]; SMEs should similarly plan for these expenses as regular and necessary.
- *Group Training:* Rather than sending employees to expensive courses, organize in-house training sessions or group up with other local SMEs to share the cost of a trainer. Inviting an expert for a half-day workshop for a group can be far more economical per business than each SME acting alone. Government agencies or industry associations might subsidize such collaborative efforts if interest is shown.
- *Cyber Insurance Evaluation:* Evaluate low-cost cyber insurance options if available in the market. While not a preventive measure, insurance can be an economic safety net that helps an SME recover financially from a major cyber incident.

Currently, uptake of cyber insurance among SMEs is very low (over 90% have not purchased it) [12], but it is worth considering as part of risk management once basic protections are in place.

- Efficient – Optimize and Maintain: Implement processes that ensure cybersecurity efforts remain efficient, up-to-date, and aligned with the SME's operations.

- *Risk-Based Focus:* Identify the most critical digital assets (e.g., customer databases, financial records) and focus protection efforts there. An efficient approach recognizes that not all data and systems are equal – prioritize securing what matters most to the business's survival and legal obligations.
- *Assign a Security Point-Person:* Even if an SME cannot hire a full-time cybersecurity officer, designate an existing employee as the point-person for cybersecurity coordination (e.g., an IT technician or tech-savvy manager). Give them basic additional training and the responsibility to track security tasks, updates, and incident response. This creates internal ownership of the process.
- *Document Simple Procedures:* Develop a concise incident response plan outlining what to do if a breach or malware infection is suspected. List key contacts (IT support provider, bank, law enforcement cyber unit), steps like isolating affected systems, and notifying customers if needed. A one-page checklist that is readily accessible can vastly improve reaction time and reduce panic during an incident.
- *Continuous Monitoring and Improvement:* Treat cybersecurity as an ongoing process. Schedule periodic check-ups – for example, quarterly reviews of user accounts and access rights, bi-annual refresher training for staff, annual security audits of the IT infrastructure (with outside help if needed). Cyber threats evolve, so SMEs must iteratively improve. Even small incremental updates (like gradually upgrading old computers or tightening network configurations) yield cumulative benefits.
- *Collaboration and Information Sharing:* Join any local business networks or online forums where threat information and solutions are shared. In Nepal, SMEs could collaborate through chambers of commerce or IT federations to stay informed about recent scams or vulnerabilities targeting businesses. Sharing experiences – such as alerting peers to a new phishing scam – is an efficient way to amplify defenses across the community.

Implementing the E3-NSME protocol should be seen as a cycle of continuous improvement. Initially, SMEs tackle the "easy" wins, then invest in economical tools and training, and finally, build routines that efficiently maintain and enhance security over time. The approach is designed to be scalable: even a micro enterprise with no IT staff can start with the Easy steps, while a larger SME can allocate more resources to cover all three aspects comprehensively.

Figure 2. Flowchart of the proposed E3-NSME cybersecurity protocol for SMEs. The process starts with the SME assessing its current cybersecurity posture, followed by implementing Easy measures (basic hygiene). Next, the company adopts Economic solutions that offer high impact for low cost. Finally, Efficient practices are put in place to optimize and sustain the security improvements. This stepwise approach enables gradual strengthening of defenses in a resource conscious manner.

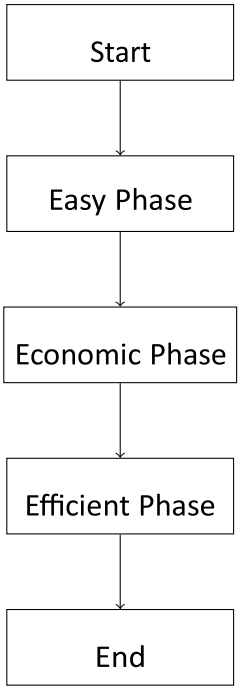

Figure 2: Flowchart of the proposed E3-NSME cybersecurity protocol for SMEs.

6 DISCUSSION

The survey results and the proposed E3-NSME protocol underscore a fundamental point: improving cybersecurity in SMEs is achievable if solutions are tailored to their context. Nepali SMEs, much like their global counterparts, struggle with awareness, expertise, and resource limitations, which have left many of them vulnerable to even relatively unsophisticated cyber threats. By systematically addressing these pain points, the E3-NSME framework offers a pathway for SMEs to enhance their security incrementally.

A key insight from this study is the critical role of awareness and education. The fact that a large majority of SMEs lack formal training and do not have incident response plans indicates that knowledge – or the lack thereof – is a root cause behind other deficiencies. This aligns with the argument by [19] that limited cybersecurity literacy is at the heart of SMEs' risk awareness and resource allocation problems. The protocol's heavy emphasis on employee awareness (Easy phase) and training (Economic phase via group training) directly tackles this root issue. If owners and staff are more aware of cyber risks and best practices, they are more likely to prioritize and implement the necessary measures.

Another discussion point is cost-effectiveness. Our findings validate that SMEs are extremely sensitive to cost, often opting to defer security expenses unless clearly justified. By outlining free and low-cost tools, and advocating collective approaches (like group workshops), we aim to demonstrate that effective cybersecurity need not be prohibitively expensive. This resonates with recommendations from international agencies: for example, ENISA's guidance for SMEs also suggests using free resources and emphasizes "cyber hygiene" as a cost-effective Défense [7, 14]. Moreover, by referencing real data (like the Markel Direct survey in the UK), we can reassure SME stakeholders that investing in measures like multi-factor authentication or staff training is not just a theoretical best practice but something that peer businesses find valuable and increasingly necessary.

It is worth comparing our proposed protocol with existing frameworks. The E3-NSME protocol has parallels with the widely cited NIST Cybersecurity Framework's core functions (Identify, Protect, Detect, Respond, Recover) but is simplified for an SME audience. For instance, our "Easy" phase corresponds to basic Protect controls and some Identify (asset awareness). The "Economic" phase focuses on Protect (with affordable tools) and some Respond (via insurance). The "Efficient" phase incorporates Detect (monitoring) and Respond/Recover (incident planning, backups). By translating such comprehensive frameworks into plain language steps, E3-NSME serves as a bridge between high-level guidelines and actionable tasks for SMEs.

A notable finding from our study is SMEs' receptiveness to external support. Unlike large firms that may view security as a competitive or proprietary concern, the SMEs in our survey were eager to collaborate and get help. This is an important cultural factor that stakeholders can leverage. Policymakers, for example, might consider establishing a national SME cybersecurity support program – perhaps a dedicated wing under the Ministry of Communication and Information Technology (MoCIT) or Nepali CERT – that provides free advisory services, threat alerts, and training modules to SMEs. The groundwork for this exists in the National Cybersecurity Policy (2016) which calls for improving access to cybersecurity information for businesses [13]. Our data provides evidence that such efforts are not only needed but would be welcomed by the SME community.

It is also instructive to reflect on the differences observed between SMEs with in-house IT expertise and those without. The disparity in adoption of measures like multi-factor authentication suggests that technical know-how is a bottleneck. This could be addressed by encouraging the development of cybersecurity-as-a-service models targeting SMEs. Already, there are startups and IT firms in other countries offering managed security services at scaled pricing for small businesses. In Nepal, promoting local IT service providers to bundle affordable security monitoring or periodic check-ups for SMEs could be part of the solution. Government incentives or public-private partnerships could jumpstart this market, ensuring quality and trust.

The E3-NSME protocol's effectiveness will ultimately depend on execution. One potential challenge is convincing SME owners to take the first step, especially if they have not yet faced a visible cyber incident. There may be a perception that implementing even "easy" measures is time-consuming or that their business is too small to matter. Overcoming this mindset might require awareness campaigns that share relatable stories of Nepali SMEs hit by cyberattacks and how simple precautions could have prevented damage. Also, demonstrating quick wins – for example, a case where an SME implemented a new backup routine and shortly after avoided data loss from a malware infection – can build confidence in the protocol.

Finally, we consider the limitations of our study in this discussion. The survey sample, while diverse, was relatively small (50 SMEs) and may not capture the full spectrum of Nepal's SME landscape. It is possible that those who responded had more interest in or awareness of cybersecurity than the average SME. This could mean the actual situation among the broader SME population is even more concerning than our results indicate. Additionally, our proposed protocol has not yet been piloted; its recommendations are drawn from best practices and the needs respondents voiced. Future work could involve implementing the E3-NSME steps in a set of SMEs as a trial and observing improvements or challenges encountered, thereby refining the protocol.

In conclusion, the discussion highlights that improving SME cybersecurity is a multi-faceted endeavour requiring engagement from the businesses themselves, support agencies, and policymakers. Our study contributes a starting point by diagnosing the problem in Nepal and offering a structured solution. The next step is turning this guidance into tangible action across the SME sector.

7 CONCLUSION AND OUTLOOK

SMEs form the backbone of Nepal's economy, and their success increasingly hinges on navigating the digital domain safely. This study has shed light on a significant vulnerability – the cybersecurity readiness gap among Nepali SMEs. We found that while SMEs are adopting digital tools and platforms, their defenses against cyber threats remain weak in critical areas. Inadequate awareness, lack of trained personnel, scarce financial resources, and absent policies create a perfect storm of exposure to cyber risks such as phishing, malware, and ransomware. These findings echo global trends but are particularly acute for Nepal as it strives to modernize its economy.

Encouragingly, our research also reveals a pathway forward. The proposed E3-NSME protocol (Easy, Economic, Efficient) provides SMEs with a clear, actionable roadmap to bolster their cybersecurity in a gradual and manageable way. By starting with simple measures, leveraging cost-effective solutions, and institutionalizing efficient practices, even the smallest of enterprises can make meaningful improvements in their cyber resilience. Importantly, this approach demystifies cybersecurity – breaking it down into practical steps that do not require extensive expertise or budgets. If widely adopted, the E3-NSME protocol could significantly reduce the incidence and impact of cyberattacks in the SME sector.

For policymakers and supporting institutions, the implications are clear. There is a need to integrate SME-focused cybersecurity support into national strategies. This could include developing standardized toolkits based on frameworks like E3-NSME, subsidizing cybersecurity audits or training for SMEs, and ensuring that information about emerging threats and solutions reaches these businesses in a timely manner (perhaps through a dedicated information portal or regular bulletins via business associations). The Nepal Rastra Bank's recent cybersecurity mandates for the financial sector are a positive step [16]; similar attention could be extended to SMEs in other sectors through guidelines or incentives that encourage better cyber practices.

Another key outlook is fostering a culture of knowledge-sharing and collaboration. As this study highlighted, SMEs are willing to learn from each other and seek help. Establishing community forums, maybe under the Federation of Nepalese Chambers of Commerce and Industry (FNCCI) or local IT clubs, where SMEs can share experiences and tips, will reinforce collective security. Cyber threats are continuously evolving – today's ransomware schemes or phishing tactics might be replaced by new threats tomorrow – so a dynamic exchange of information will be crucial in keeping defenses up to date.

Looking ahead, further research should be conducted to refine our understanding of SME cybersecurity in Nepal. A larger nationwide survey would be valuable to quantify the state of affairs more precisely. Additionally, qualitative case studies on SMEs that have successfully improved their cybersecurity (or conversely, those that suffered major breaches) would provide deeper insight into effective strategies and common pitfalls. Measuring the effectiveness of implementing the E3-NSME protocol in a pilot program could also provide data to fine-tune the recommendations and demonstrate concrete results, which in turn can motivate broader adoption.

In conclusion, as Nepali SMEs continue to embrace digital innovation, it is imperative that cybersecurity is not left behind as an afterthought. The cost of inaction is high – a single cyber incident can undo years of hard-earned business progress. By proactively adopting a culture of cyber safety, supported by frameworks like E3-NSME and aided by government and community support, SMEs in Nepal can confidently turn digital challenges into opportunities. A secure digital foundation will not only protect these businesses but also enhance their competitiveness and trustworthiness in an increasingly connected marketplace. The time to act is now, and the tools to do so are within easy reach.

Acknowledgements

The author extends sincere thanks to Dr. Pawan (Lincoln University College) for their invaluable guidance and support throughout this research. Their feedback greatly improved the quality of this work. Appreciation is also due to the SME owners and employees who participated in the survey, for sharing their experiences and insights.

REFERENCES

1) Adhikari, S. N., & Molla, N. (2024). Navigating the digital shift: Exploring the impact of technology on management practices in small and medium enterprises (SMEs) in Nepal. *Nepalese Journal of Management and Technology, 2*(2), 91–109. https://doi.org/10.3126/njmt.v2i2.68730
2) Ahmad, A., Maynard, S. B., & Park, S. (2019). Information security strategies: Towards an organizational multi-strategy perspective. *Journal of Intelligent Manufacturing, 30*(3), 1103–1116. https://doi.org/10.1007/s10845-017-1314-3
3) Alshaikh, M., Maynard, S., Ahmad, A., & Chang, S. (2021). Cybersecurity awareness for SMEs: A systematic literature review. *Information & Computer Security, 29*(1), 72–100. https://doi.org/10.1108/ICS-06-2020-0091
4) Bada, A., & Sasse, M. A. (2015). Cybersecurity for small and medium-sized enterprises: Best practices and guidelines. Springer. https://doi.org/10.1007/978-3-319-13907-7
5) Bishop, M. (2018). *Computer security: Art and science* (2nd ed.). Addison-Wesley.
6) Central Bureau of Statistics (CBS). (2020). *National Economic Census 2018, National Report*. Kathmandu: Government of Nepal.

7) European Union Agency for Cybersecurity (ENISA). (2020). *Cybersecurity for SMEs: Challenges and recommendations*. ENISA Publications. https://www.enisa.europa.eu/publications/cybersecurity-for-smes
8) Gonzalez, G., & Blackwell, T. (2021). *Cybersecurity for SMEs: Challenges and solutions*. Wiley.
9) Gundu, T., & Flowerday, S. V. (2021). The effectiveness of cybersecurity awareness training for SMEs. *Computers & Security, 108*, 102364. https://doi.org/10.1016/j.cose.2021.102364
10) Gupta, A., & Hammond, R. (2020). SMEs and cybersecurity: Threats, challenges, and strategies. *International Journal of Business Continuity and Risk Management, 10*(2/3), 151–166. https://doi.org/10.1504/IJBCRM.2020.100321
11) Kabanda, S., Tanner, M., & Kent, C. (2018). Exploring SME cybersecurity practices in developing countries. *Journal of Organizational Computing and Electronic Commerce, 28*(3), 266–282. https://doi.org/10.1080/10919392.2018.1480380
12) Markel Direct UK. (2024). *SME cybersecurity statistics 2024*. https://www.markeldirect.co.uk/blog/sme-cybersecurity-statistics-2024
13) Ministry of Communication and Information Technology (MoCIT). (2016). *National Cybersecurity Policy 2016 (Draft)*. Kathmandu: Government of Nepal.
14) National Institute of Standards and Technology (NIST). (2020). *Cybersecurity Framework Version 1.1*. NIST Publications. https://www.nist.gov/cyberframework
15) Nepal Rastra Bank (NRB). (2019). *SMEs Financing in Nepal*. Kathmandu: Nepal Rastra Bank.
16) Nepal Rastra Bank (NRB). (2025). Revised Cybersecurity Framework guidelines (Mandates for Banks and Financial Institutions). (As reported in NepalNews, Nov 2025). https://www.nrb.org.np/contents/uploads/2025/01/Payment-Oversight-Report-2023-24.pdf
17) Nepal Telecommunications Authority (NTA). (2016). *Cybersecurity awareness campaigns*. Kathmandu: Government of Nepal.
18) Organisation for Economic Co-operation and Development (OECD). (2021). *OECD SME and Entrepreneurship Outlook 2021*. OECD Publishing.
19) Rombaldo Junior, C., Becker, I., & Johnson, S. (2023). Unaware, unfunded and uneducated: A systematic review of SME cybersecurity. arXiv:2309.17186 [cs.CR].
20) Sharma, D. R., Joshi, S. P., & Shakya, M. (2025). Competitive strategies on the performance of small and medium-sized enterprises in Nepal. *Journal of Service, Innovation and Sustainable Development, 6*(1), 33–49.
21) Srinivas, J., Das, A. K., & Kumar, N. (2022). Cloud computing security challenges for SMEs. *Journal of Network and Computer Applications, 199*, 103299.https://doi.org/10.1016/j.jnca.2021.103299
22) Team Ninja. (2025). 7 SMB cybersecurity statistics you need to know in 2025. *NinjaOne Blog*. https://www.ninjaone.com/blog/smb-cybersecurity-statistics/
23) Verizon. (2019). *2019 Data Breach Investigations Report*. Verizon Business.