NPRC Journal of Multidisciplinary Research
Volume 3, Issue 3, March, 2026 Pages: 58-67
ISSN: 3059-9148 (Online)
DOI: 10.3126/nprcjmr.v3i3.91898

OPEN ACCESS

Modern Cybersecurity Technology Adoption in Nepal

Sijan Bhattarai
Thapathali Engineering Campus, Kathmandu, Nepal
sijan.762419@thc.tu.edu.np
https://orcid.org/0009-0002-6532-2126

Received: February 10, 2026 Revised & Accepted: March 27, 2026

Abstract

Background: Rapid growth in internet connectivity, digital banking, and online services has accelerated Nepal's digital transformation in recent years. While this expansion has improved financial inclusion and service delivery, it has also exposed critical vulnerabilities in national cyber infrastructure. Increasing cybercrime incidents, weak cybersecurity awareness, and limited technical capacity have made cybersecurity a growing national concern, particularly for banking, government, and business sectors.

Methods: This study employed a descriptive and analytical design with a case-based exploratory approach to examine cybersecurity technology adoption in Nepal across SOC, offensive security, and GRC domains. Primary data were collected through structured interviews with senior and mid-level engineers from cybersecurity companies via email, LinkedIn, and in-person or virtual meetings. Discussions focused on tools, technologies, operational practices, and implementation challenges. Secondary data were obtained from government reports, academic literature, regulatory publications, and global cybersecurity indices to contextualize cyber threats and policy frameworks. Access to detailed technical information was limited due to confidentiality and organizational policies; findings reflect high-level insights validated with company representatives. Data were analyzed descriptively and comparatively to identify common patterns, technological trends, and gaps in cybersecurity adoption across organizations.

Results: Nepal has made measurable progress in foundational cybersecurity, ranking Tier 3 in the Global Cybersecurity Index 2024. Common threats include phishing, ransomware, malware, social engineering, and web application exploitation, fueled by weak system configurations, low user awareness, and limited law enforcement. Leading firms are adopting technologies like SIEM monitoring, anomaly detection, network analysis, vulnerability assessments, penetration testing, endpoint security, and compliance frameworks (PCI DSS, ISO). Adoption remains uneven due to skill shortages, funding constraints, and policy gaps.

NPRC Journal of Multidisciplinary Research
Volume 3, Issue 3, March, 2026 Pages: 58-67
ISSN: 3059-9148 (Online)
DOI: 10.3126/nprcjmr.v3i3.91898

Conclusion: Nepal's cybersecurity is evolving but still unprepared for advanced threats. Strengthening coordination, developing skilled workforce, deploying automated solutions, and enforcing cyber policies are essential. Context-specific, scalable strategies are key to enhancing the country's digital resilience.
Novelty: This study provides a consolidated analysis of cybersecurity threats, technologies challenges, and policy initiatives in Nepal while presenting real-world insights from domestic cybersecurity companies offering understanding of Nepal's current cyber readiness.
Keywords: End Point Security, Penetration Testing, Vulnerability Assessment, SIEM

Introduction

Nepal is a small landlocked country where access to basic infrastructure such as electricity has not yet reached every household. However, internet connectivity has grown rapidly in recent years. In 2072, Internet penetration stood at 47.24 percent, and by 2024 total broadband subscriptions exceeded 140 percent. According to Nepal Rastra Bank, the number and value of online payments using cards increased by 48.90 percent and 42.61 percent respectively in fiscal year 2023-24 compared to fiscal year 2022-23. From fiscal year 2022-23, internet banking users increased by 8.23 percent, while mobile banking users grew significantly by 59.13 percent. Along with this expansion, a large number of cyber threats have also emerged.

With the growth of the digital economy and digital systems, the number of cybercrime incidents has been increasing every year. According to Nepal Police, a total of 19,730 cybercrime complaints were filed in fiscal year 2080-81, representing a 119 percent increase compared to fiscal year 2079-80. Among the affected population, 44.32 percent were women, 3.2 percent were children, and 3.8 percent were individuals from the LGBTQI+ community. Koshi Province recorded the highest number of cybercrime cases at 1,149, while Sudurpashchim Province reported the lowest number with only 60 cases.

These trends highlight that cybersecurity has become a critical concern in Nepal that is rapidly digitizing. In Nepal, cybersecurity is especially important due to the fast and largely unprotected digital transformation of the banking, government, and business sectors. Effective cybersecurity measures are essential to protect financial assets, secure personal and institutional data, and maintain public trust in digital services. Major cyber threats faced by Nepal include phishing attacks, ransomware, and website hacking.

Research Objective

The main objective of this study is to analyze the current state of cybersecurity technology adoption in Nepal by examining the tools, practices, and challenges within leading domestic cybersecurity firms, thereby providing a consolidated assessment of the nation's cyber readiness.

Common Cyber Threats in Nepal

Nepal's current cybersecurity standing in the Global Cybersecurity Index 2024 places the country in Tier 3, indicating noticeable progress in establishing foundational cybersecurity

NPRC Journal of Multidisciplinary Research
Volume 3, Issue 3, March, 2026 Pages: 58-67
ISSN: 3059-9148 (Online)
DOI: 10.3126/nprcjmr.v3i3.91898

measures while also highlighting significant gaps in technical capacity, inter-institutional cooperation, and skilled workforce development. Despite these improvements, Nepal continues to face a wide range of cyber threats that challenge the security of its digital ecosystem.

Commonly observed cyber threats in Nepal include network reconnaissance and exploitation techniques such as packet sniffers, ping sweeps, port scanning, phishing, and SQL injection attacks (Bhagat, 2023). These attacks largely exploit weak network configurations, unpatched systems, and low levels of user awareness. Incidents are frequently reported across government institutions, educational organizations and small to medium enterprises, indicating systemic vulnerabilities in both public and private sectors.

Beyond technical attacks, Nepal is increasingly affected by social engineering and cyber-enabled crimes. Phishing based financial fraud, social media impersonation, online harassment, identity theft and malware infections are among the most prevalent threats impacting individuals and businesses (Maharjan, 2023). The rapid expansion of digital banking, e-commerce and social media usage, combined with limited cybersecurity awareness and weak enforcement mechanisms, has significantly expanded the national attack surface (Lohani & Kumar, 2024). Addressing these challenges requires strengthened legal frameworks, improved technical safeguards, enhanced public awareness initiatives and coordinated national cybersecurity strategies (Gupta, 2024).

In contrast, existing cyber laws and policies remain poorly implemented, while internal political instability and external geopolitical pressures further exacerbate cyber risks. Strengthening the national cybersecurity strategy, improving institutional coordination and ensuring the protection of critical information infrastructure are therefore essential for Nepal's digital and economic resilience (Giri, 2019). Overall, Nepal faces a growing volume of cyber threats while lacking effective implementation of cybersecurity laws, policies and institutional capacity, leaving its critical infrastructure and digital systems highly vulnerable (Ghimire, 2023).

Technologies adopted in Nepal

Globally, technologies such as artificial intelligence and machine learning, cloud security solutions, multi-factor authentication, and data encryption and secure networks are being widely adopted to strengthen cybersecurity. Organizations across industries are using AI and machine learning to detect threats faster, identify unusual behavior, and respond to cyber attacks in real time. As more systems move to the cloud, cloud security solutions help protect data, applications, and infrastructure from evolving risks. Multi-factor authentication has become a standard practice to reduce unauthorized access by adding extra layers of identity verification. At the same time, data encryption and secure networks ensure that sensitive information remains protected during storage and transmission. Together, these technologies play a critical role in addressing modern cyber threats and improving global digital security. The extent and maturity of adoption vary significantly in developing countries such as Nepal due to differences in political, social, and economic factors, as well as available resources (Zwarts et al., 2025).

NPRC Journal of Multidisciplinary Research
Volume 3, Issue 3, March, 2026 Pages: 58-67
ISSN: 3059-9148 (Online)
DOI: 10.3126/nprcjmr.v3i3.91898

To understand the current state of technology adoption, a case based analysis of selected cybersecurity companies in Nepal was conducted. The findings are summarized in Table 1.

Table 1
Comparison of Cybersecurity Technology Adoption in Nepal

Company	Primary Focus	Key Technologies	Security Domain	Notable Capability
Cryptogen	SOC + Offensive + GRC	SIEM, Wireshark, Shodan, Nmap	Hybrid	Log analysis, incident response, compliance, alignment
Threatnix	Offensive	Burp Suite, Nmap	Penetration Testing	Web and network vulnerability assessment
SecurityPal	GRC	AI driven automation	Compliance	Security questionnaire and assurance automation
Vairav Tech	SOC + Offensive	TridentSOC, Wazuh, Burp Suite, Sophos	Hybrid	SOC as a service with real time monitoring
CodeAvatar	Offensive+ Defensive	Burp Suite, custom tools, firewall systems	Hybrid	Manual pentesting and internal security operations
Green Tick	Threat intelligence	AI crawlers, dark web, monitoring tools	Intelligence	Data leak detection and exposure monitoring

Source: Survey, 2026

NPRC Journal of Multidisciplinary Research
Volume 3, Issue 3, March, 2026 Pages: 58-67
ISSN: 3059-9148 (Online)
DOI: 10.3126/nprcjmr.v3i3.91898

Analysis of Technology Adoption

The analysis reveals several important patterns in Nepal's cybersecurity ecosystem. A dominant trend is the strong emphasis on offensive security practices, particularly penetration testing and vulnerability assessment. Tools such as Burp Suite and Nmap are widely used across multiple organizations, indicating that proactive identification of system vulnerabilities through simulated attacks remains a primary focus in the industry.

In comparison, the adoption of defensive security mechanisms such as Security Operations Center based monitoring and SIEM systems is still developing. Only a limited number of companies, including Cryptogen and Vairav Tech, demonstrate relatively mature capabilities in continuous monitoring, incident detection, and response. This suggests that while defensive security practices are emerging, they are not yet consistently implemented across all organizations.

Compliance-oriented services appear to be less widespread but are gradually gaining importance. Companies such as SecurityPal specialize in security assurance and third party risk management, leveraging automation and artificial intelligence to handle large scale security assessments. This reflects a growing demand for compliance driven cybersecurity solutions, particularly in international business environments.

Another key observation is the gradual integration of artificial intelligence and automation in cybersecurity operations. These technologies are primarily applied in areas such as threat intelligence, anomaly detection, and security response. However, adoption remains uneven, with many organizations continuing to rely on manual processes and traditional tools due to limitations in technical expertise, financial resources, and infrastructure.

Additionally, variations in organizational focus indicate a fragmented cybersecurity landscape, where companies tend to specialize in specific domains such as offensive security, SOC operations, or compliance rather than offering fully integrated solutions. This fragmentation highlights both the opportunities and challenges in developing a mature and comprehensive cybersecurity ecosystem in Nepal.

Overall, the findings suggest that while Nepal has begun adopting modern cybersecurity technologies, the level of maturity varies significantly across organizations. The ecosystem is characterized by strong offensive security capabilities, emerging defensive practices, and limited but growing adoption of automated and compliance driven solutions.

Challenges in Technology Adoption

The findings suggest that existing cybersecurity guidance largely derived from developed nations is poorly suited to countries with emerging ICT infrastructures. By examining cases from Rwanda and Tunisia, it highlights the importance of adopting context-specific, affordable and rapidly implementable cybersecurity strategies rather than relying on one size fits all models (Target, 2010).

In the context of Nepal, the national literacy rate remains below 80 percent. Although internet and mobile access is widespread, only a small proportion of users possess adequate awareness of cybersecurity risks and threats. A study published in (Gurung et al., 2023) surveyed 157 teachers and found that 47 percent of respondents were either fully or partially unaware of the

NPRC Journal of Multidisciplinary Research
Volume 3, Issue 3, March, 2026 Pages: 58-67
ISSN: 3059-9148 (Online)
DOI: 10.3126/nprcjmr.v3i3.91898

risks associated with using online resources. Furthermore, 33 percent of the respondents reported using fraudulent websites to stream movies or download digital content, indicating risky online behavior even among educated professionals.

Nepal's current laws and policies are not sufficiently robust to address the rapidly evolving technological landscape and the increasingly sophisticated nature of cyber threats. Existing policies place greater emphasis on expanding access to digital services than on protecting systems, data and users from cyber risks (Acharya & Dahal, 2021). This imbalance weakens the overall cybersecurity posture of the country.

Additionally, Nepal faces a significant shortage of skilled cybersecurity professionals. Both government institutions and private sector organizations often fail to allocate adequate funding for cybersecurity initiatives, limiting their ability to upgrade technologies and conduct regular security assessments. As cyber threats continue to evolve, Nepal cannot rely on outdated and manual approaches to cyber defense and must transition toward implementing automated and proactive cybersecurity systems to enhance national digital resilience.

Government Policies and Initiatives

Nepal has been increasingly active in developing its cyber legal and policy framework to address rising digital threats and protect citizens, institutions, and national infrastructure. The country has enacted foundational cyber laws and regulations, including provisions under the *Electronic Transactions Act* and related bylaws that criminalize unauthorized access, identity theft, and other cyber offenses, while broader legislation such as the *Information Technology and Cybersecurity Bill* (in progress) seeks to modernize protections and penalties for contemporary cybercrimes. In 2023, the government approved the *National Cyber Security Policy*, which outlines a comprehensive roadmap for strengthening cyber defenses, enhancing digital literacy, and fostering collaboration across public, private, and academic sectors to build a resilient cyberspace. To operationalize these policy goals, Nepal is establishing a *National Cybersecurity Center* tasked with coordinating monitoring, incident response, awareness, and preparedness, and initiatives from institutions like CSRI Nepal and NAS-IT's cybersecurity committee supplement national efforts by providing research, training, and multi-stakeholder engagement. Recent regulatory measures also include directives for social media platforms to register locally to ensure accountability, reflecting a broader push to enforce compliance and curb harmful online activity.

Despite these developments, the effectiveness of policy implementation remains limited. Prior studies by Nepali researchers highlight that although legal provisions exist, they are often outdated, insufficient, or inadequately enforced to address modern cyber threats (Sushant Acharya & Sudhamshu Dahal, 2021). Their findings indicate that the lack of updated policies, low awareness, and weak enforcement mechanisms significantly increase cybersecurity risks in Nepal. Similarly, research by (Basanta Prasad Adhikari et al., 2025) identifies resource limitations, insufficient skilled manpower, and weak institutional capacity as key barriers to effective cybersecurity practice and policy execution in Nepal.

Furthermore, broader policy analyses suggest that Nepal's security framework still lacks adequate focus on non-traditional threats such as cybersecurity, with institutional and strategic

NPRC Journal of Multidisciplinary Research
Volume 3, Issue 3, March, 2026 Pages: 58-67
ISSN: 3059-9148 (Online)
DOI: 10.3126/nprcjmr.v3i3.91898

gaps limiting effective response (Ishwor Budhathoki, 2024). While initiatives such as the proposed National Cybersecurity Center and contributions from organizations like CSRI Nepal and NAS-IT indicate positive progress, implementation remains in early stages.

Overall, the cybersecurity landscape in Nepal continues to reflect a gap between policy formulation and effective implementation. Addressing this gap requires stronger institutional coordination, updated legal frameworks, investment in skilled human resources, and improved enforcement mechanisms.

Future Opportunities

The global cybersecurity market is projected to expand significantly over the coming decade, reflecting rising digital adoption and increasingly sophisticated cyber threats. According to market research, the global cybersecurity market was valued at approximately USD 301.9 billion in 2025 and is expected to reach around USD 878.48 billion by 2034, growing at a compound annual growth rate (CAGR) of about 12.6 % from 2025 to 2034. Another forecast estimates the market will grow from about USD 206.8 billion in 2024 to USD 352.5 billion by 2030, at a CAGR of 9.3 % during 2024–2030. This robust global growth is driven by the rising number of cyberattacks, cloud adoption, AI-enabled threats, and increasing regulatory and compliance requirements.

In Nepal, although the overall cybersecurity market is much smaller in absolute terms, it is also expanding rapidly as the country's digital economy grows and cyber risks increase. Statista forecasts the Nepal "cyber solutions" market will reach about USD 15.82 million by 2025 and grow at a CAGR of approximately 11.62 % from 2025 to 2030 to reach around USD 27.41 million by 2030. In addition, other projections suggest Nepal's cybersecurity market could reach about USD 34.09 million by 2025 with around 12.5 % annual growth. These trends are propelled by increasing internet penetration, digital payment adoption, and government policy initiatives to strengthen national cyber defenses.

This means that while the scale differs dramatically, the growth trajectory in Nepal reflects global cybersecurity expansion, indicating rising demand for security technologies, skilled professionals, and institutional readiness to address emerging cyber threats locally.

Discussion

The results demonstrate Nepal's cybersecurity landscape in the context of rapid digital transformation and increasing cyber threats. The findings show that although Nepal has made measurable progress in developing policies and foundational cybersecurity structures, significant gaps remain in technical capacity, enforcement mechanisms, skilled workforce development, and institutional coordination. Consistent with previous studies such as Bhagat (2023) and Maharjan (2023), phishing, ransomware, social engineering, and system exploitation remain the most prevalent threats, largely driven by weak configurations, low cybersecurity awareness, and limited implementation of cyber laws. The study further extends earlier research by incorporating insights from domestic cybersecurity companies, revealing gradual adoption of modern technologies such as SIEM monitoring, vulnerability assessment,

NPRC Journal of Multidisciplinary Research
Volume 3, Issue 3, March, 2026 Pages: 58-67
ISSN: 3059-9148 (Online)
DOI: 10.3126/nprcjmr.v3i3.91898

penetration testing, and compliance frameworks, though adoption remains uneven due to financial and human resource constraints.

Cost and resource constraints play a critical role in the uneven adoption of cybersecurity technologies in Nepal. Advanced solutions such as Security Information and Event Management (SIEM) platforms, automated threat detection systems, and modern network architectures such as Software Defined Networking (SDN) require substantial investment in infrastructure, licensing, and ongoing maintenance. Many organizations, particularly small and medium-sized enterprises, lack the financial capacity to sustain such investments. In addition, the limited availability of skilled cybersecurity professionals further constrains adoption, as these technologies demand specialized expertise for deployment, configuration, and real-time management. Infrastructure limitations, competing organizational priorities, and relatively weak regulatory enforcement further reduce the urgency for adopting advanced security frameworks. Consequently, many organizations continue to rely on traditional tools and manual practices, resulting in fragmented and inconsistent implementation of modern cybersecurity technologies.

The reliance on tools such as Burp Suite and Nmap for offensive security assessments generally reflects a low to moderate level of organizational maturity. While these tools are effective for web application testing and network scanning, their predominant use indicates a tool-centric and potentially reactive approach to security. This often leads to limited coverage across other critical domains, including cloud, mobile, and internal systems. In contrast, a more mature offensive security framework typically incorporates a broader range of specialized tools, standardized methodologies, comprehensive documentation, and continuous improvement practices, enabling a more proactive and systematic security posture.

Despite these systemic challenges, certain organizations have demonstrated the ability to operate at a global scale. For instance, SecurityPal effectively serves Fortune 500 companies by focusing on security assurance and compliance rather than conventional offensive or defensive operations. By integrating AI-driven automation with expert human analysis, the company is able to process large volumes of security questionnaires, vendor assessments, and regulatory requirements efficiently. Its 24/7 operational model, supported by certified professionals, enables consistent delivery of high-quality, standardized outputs, thereby overcoming local constraints related to skilled workforce and infrastructure. This specialized approach allows global enterprises to meet complex compliance requirements without being significantly affected by regional limitations.

Similarly, the adoption of proprietary tools such as TridentSOC by Vairav Tech illustrates an alternative approach to addressing resource constraints. Proprietary solutions typically offer integrated interfaces, vendor support, and pre-configured workflows, which reduce the need for extensive in-house expertise and simplify deployment. In contrast, open-source solutions such as Wazuh provide greater flexibility and cost advantages but require higher technical proficiency for configuration, maintenance, and optimization. The choice between proprietary and open-source tools therefore reflects a trade-off between ease of use and operational support on one hand, and cost efficiency and customization on the other.

NPRC Journal of Multidisciplinary Research
Volume 3, Issue 3, March, 2026 Pages: 58-67
ISSN: 3059-9148 (Online)
DOI: 10.3126/nprcjmr.v3i3.91898

Conclusion and Recommendation

In conclusion, Nepal's cybersecurity ecosystem is evolving but remains insufficiently prepared to address the growing scale and sophistication of cyber threats. While progress has been made in policy formulation and institutional recognition, practical implementation, automation, and sector-wide compliance remain limited. This study contributes new knowledge by integrating threat trends, policy analysis, and real-world industry practices to provide a consolidated assessment of Nepal's current cyber readiness. To strengthen national digital resilience, Nepal should prioritize stronger enforcement of cybersecurity policies, invest in education and professional training, mandate regular security audits for critical infrastructure, promote public-private collaboration, and increase funding for modern automated security technologies.

Author Contribution

The author was solely responsible for the conceptualization of the study, literature review, data collection from secondary sources, case-based analysis of cybersecurity companies, interpretation of findings, and preparation and revision of the manuscript.

Transparency Statement: The author confirms that this study has been conducted with honesty and in full adherence to ethical guidelines.
Data Availability Statement: Author can provide data which are publicly available
Conflict of Interest: The author declares there is no conflict of interest.

NPRC Journal of Multidisciplinary Research
Volume 3, Issue 3, March, 2026 Pages: 58-67
ISSN: 3059-9148 (Online)
DOI: 10.3126/nprcjmr.v3i3.91898

References

Acharya, S., & Dahal, S. (2021). Security threats and legalities with digitalization in Nepal. Research *Nepal Journal of Development Studies*. 4(2), 1-15. https://doi.org/10.3126/rnjds.v4i2.42666

Adhikari, B. P., Ale, K., & Bhusal, M. P. (2025). Understanding the key factors influencing cybersecurity practices in Nepalese organizations. *OCEM Journal*. 4(1), 194–208. https://doi.org/10.3126/ocemjmtss.v4i1.74761

Bhagat, C. K. (2023). Study of Current Cybersecurity Threats to Information & Operational Technology (IOT) and their Effect on e-Governance in Nepal. *Journal of UTEC Engineering Management*, 1(1), 41-50. https://doi.org/10.36344/utecem.2023.v01i01.005

Budhathoki, I. (2025). Re-conceptualizing Nepal's Security Policies: A Comprehensive Framework for Addressing Non-Traditional Security Threats. *The Shivapuri Journal*, *26*(1), 79–93. https://doi.org/10.3126/shivapuri.v26i1.75835

Dhungana, R.K., Gurung, L., & Poudyal, H. (2023). Cybersecurity Challenges and Awareness of the Multi-Generational Learners in Nepal. *Journal of Cybersecurity Education, Research and Practice*, 2023(2). https://digitalcommons.kennesaw.edu/jcerp/vol2023/iss2/5

Ghimire, K. (2023). Cyber-Attack Issues: Laws & Policies and the Role of Librarians. *An International Journal of Nepal Library Association*, 2, 206-234. https://doi.org/10.3126/access.v2i01.59002

Giri, S. (2019). Cyber Crime, Cyber threat, Cyber Security Strategies and Cyber Law in Nepal. *Pramana Research Journal*, 9(3). https://pramanaresearch.org/

Gupta, L. (2024). Issues of Cyber security and its solutions in Nepalese Context. *NPRC Journal of Multidisciplinary Research*, 1(2), 122-127. https://doi.org/10.3126/nprcjmr.v1i2.69333

Lohani, A., & Kumar, S. (2024). Impact of Cyber Security Awareness Among Higher Studies: Case Study of Nepal. *LBEF Research Journal of Science, Technology and Management*, 6(1).

Maharjan, A. (2023). A Study of Scams and Frauds using Social Engineering in "The Kathmandu Valley" of Nepal. *University of Turku*.

Target, A. C. (2010). Cybersecurity Challenges in Developing Nations. *Carnegie Mellon University, Department Engineering and Public Policy*.

Zwarts, H., Du Toit, J., & Von Solms, B. (2025). Augmenting cybersecurity awareness at critical infrastructures in developing countries through a cybersecurity governance maturity model. Proceedings of the 24th European Conference on Cyber Warfare and Security (ECCWS 2025), *Academic Conferences International*. https://doi.org/10.34190/eccws.24.1.3708