Impact of Cyber Security Awareness Among Higher Studies: Case Study of Nepal

Ankit Lohani[1], Er Sudhir Kumar[2]
[1]PG Scholar, Lord Buddha Education Foundation, Kathmandu, Nepal
[2]Lecturer, Patan College for Professional Studies, Lalitpur, Nepal

ABSTRACT

As Nepal continues to advance technologically, the academic sector must confront the challenges posed by cyber threats head-on, fostering an environment that not only harnesses the benefits of digitalization but also prioritizes the protection of sensitive information and the overall well-being of the academic community. This research delves into the crucial realm of cybersecurity awareness among Higher Education stakeholders in Nepal. Through a quantitative survey approach, the study assesses the level of cybersecurity awareness, Cyber security knowledge, and practices among students, faculty, and administrators in Nepalese universities. The findings not only reveal the current status of cybersecurity awareness but also highlight pertinent challenges and opportunities for enhancing awareness and promoting secure behavior. By identifying key factors influencing cybersecurity awareness and evaluating the effectiveness of existing cybersecurity training programs, this research contributes valuable insights to the field. The study's recommendations offer actionable strategies for policymakers, educational institutions, and cybersecurity professionals to bolster cybersecurity awareness efforts and safeguard the academic community against evolving cyber threats.

Keywords: *Cyber security Awareness (C.A), Higher studies, Cyber security Knowledge, Cyber security attitude, Self-Perception of skills, Higher Education (H.E)*

1. Introduction

According to (Rawindaran, 2023) and (Maharjan & Chatterjee, 2019), in an era marked by rapid technological advancements and heightened digital connectivity, the significance of cybersecurity has emerged as a critical concern, particularly within the realm of H.E. With the proliferation of online platforms and the integration of information and communication technologies (ICT) into academic landscapes, institutions of higher studies in Nepal find themselves at the forefront of a dynamic digital landscape. The evolving cyber threat landscape necessitates a comprehensive understanding of C.A and its profound implications on the safety, privacy, and academic pursuits of students and faculty members. This thesis seeks to explore and analyze the impact of C.A among H.E stakeholders in Nepal. By delving into the multifaceted dimensions of C.A, encompassing knowledge, behaviors, attitudes, and educational initiatives, this research aims to contribute valuable insights into the effectiveness of current cybersecurity measures and the areas requiring attention and enhancement (Ikhalia et al., 2019). This study is situated within the broader framework of global cybersecurity discourse while specifically addressing the unique context of higher education in Nepal. Through an empirical investigation, including surveys, interviews, and data analysis, this research endeavors to ascertain the existing level of C.A among students, faculty, and administrative staff in H.E institutions. Furthermore, the study aims to identify potential gaps in awareness, discern the impact of current awareness programs, and propose strategic recommendations for enhancing cybersecurity resilience within the academic landscape of Nepal.

2. Problem Statement

Despite the increasing reliance on digital technologies in higher education institutions in Nepal, there remains a significant gap in understanding the level of cybersecurity awareness among stakeholders, including students, faculty, and administrative staff. This gap poses a considerable risk as it leaves academic institutions vulnerable to cyber threats, including data breaches, identity theft, and cyber-attacks. Moreover, the lack of comprehensive cyber security awareness initiatives tailored to the Nepalese higher education context further exacerbates this vulnerability. Therefore, there is a pressing need to investigate and analyze the current state of cyber security awareness, identify potential gaps, and propose targeted strategies to enhance cybersecurity resilience within the academic landscape of Nepal (Rawindaran, 2023).

3. Research Questions

i. What is the relationship between cyber security knowledge and cyber security attitude in the education sector?

ii. How does self-perception of skill relate to cyber security attitude?

iii. What is the relationship between actual skill and behaviors and cybersecurity attitude?

4. Objectives

i. To examine the relationship between cyber security knowledge and cyber security attitude in education sector.

ii. To examine the relationship between self-perception of skill and cyber security attitude.

iii. To examine the relationship between actual skill and behaviors and cybersecurity attitude.

5. Scope of the Study

The research explores the impact of cybersecurity awareness among stakeholders within higher education institutions in Nepal. It seeks to understand the levels of cyber security among, knowledge, and practices among students, faculty, and administrators. Additionally, the study aims to identify factors influencing cyber security awareness and proposes recommendations for enhancing cybersecurity initiatives in higher education institutions.

While the study aims to uncover cyber security attitudes within Nepal's higher education sector, several limitations should be noted. Firstly, findings may not be universally applicable beyond Nepal due to cultural, technological, and regulatory variations. Secondly, sampling constraints, such as limited resources and participant accessibility, may impact the study's generalizability. Lastly, time limitations might restrict the depth of examination into all aspects of cyber security knowledge. These constraints underscore the need for cautious interpretation and consideration of contextual differences.

6. Literature Review

A brief account of a study was conducted to analyse C.A (CSA) levels among students at a private higher education institution in South Africa (Chandarman & Niekerk, 2017) . The study used a questionnaire to assess students on four critical dimensions: cybersecurity knowledge, self-perception of cybersecurity skills, actual cybersecurity skills and behaviour, and cybersecurity attitudes. The findings found disparities and instances of "cognitive dissonance" between these factors, indicating that pupils may be vulnerable to cyber-attack. The study emphasizes the importance of customized CSA programs that address specific shortcomings observed among distinct user categories.

In recent times, banks have transitioned to relying on information-based IT systems to manage wealth in the form of data, posing a significant challenge of safeguarding against cyber-attacks in Nepal's banking sector. With cyber-attacks increasing in frequency and complexity, there is a pressing need for adaptable countermeasures to mitigate risks promptly. This study intends to provide a framework based on the key principles of the National Institute of Standards and Technology (NIST) to proactively reduce cyber security risks in Nepalese banking. The framework aims to improve resilience against new threats, provide prompt response, and encourage recovery in the case of an incident by following the Identify, Protect, Detect, Respond, and Recover principles. The framework aims to improve Nepal's banking sector's overall security posture by implementing specific cyber security practices and using suitable security technologies. This will protect key data and assets from any cyber-attacks (Maharjan & Chatterjee, 2019).

In the realm of smart-home technology, C.A among users is a critical yet understudied area. While smart-home systems offer convenience and efficiency, they also present multifaceted security challenges spanning devices, networks, and cloud servers. However, scant research focuses on understanding the attitudes and behaviors of smart-home users towards cybersecurity. Addressing this gap, this paper delves into the potential interests of adult smart-home users in C.A training and explores nonfinancial incentives that could incentivize them to adopt secure practices. Through a survey questionnaire administered to 423 smart-home users aged 25 to 64, including participants from Japan and the UK, the study sheds light on cultural influences on users' attitudes towards cybersecurity. Cultural factors significantly impact willingness to participate in training, views on the importance of training for children and seniors, and preferences for nonfinancial incentives. The findings underscore the importance of considering cultural nuances when designing cybersecurity programs for smart-home users and highlight the need for cost-effective and culturally sensitive awareness training initiatives. Additionally, the study offers insights for policymakers on establishing nonfinancial incentives to promote cybersecurity practices among smart-home users, thereby contributing to a deeper understanding of C.A in smart-home environments (Douha et al., 2023).

Alaqahtani (2022) assessed the level of C.A among college students, particularly at Imam Abdurrahman Bin Faisal University. The research examines three critical aspects: password security, browser security, and social media practices. A module is developed to enhance students' understanding of cybersecurity, and a survey is conducted to evaluate their awareness levels. Statistical analyses, including validity and reliability tests, correlation tests, multiple regression, and ANOVA tests, are employed to analyze the survey responses. The results indicate that password security, browser security, and social media activities significantly influence C.A among students, as evidenced by the statistical tests conducted. The findings suggest that students have recognized the importance of C.A. This literature review underscores the significance of assessing C.A among college students and highlights the key factors contributing to their understanding of cybersecurity practices, including password security, browser security, and social media usage.

Senthilkumar & Easwaramoorthy (2017) analyzed the level of C.A among college students in Tamil Nadu,India with a specific focus on various internet security threats. In recent years, cybercrime has emerged as a significant challenge affecting areas such as national security, public safety, and personal privacy. To mitigate the risk of falling victim to cybercrime, it is essential for individuals to be well-informed about security measures to safeguard themselves. To achieve this objective, a well-structured questionnaire survey method will be employed to analyze college students' awareness of cyber security issues. The survey will be conducted in major cities across Tamil Nadu,India targeting various security threats prevalent on the internet, including email scams, viruses, phishing attempts, fake advertisements, popup windows, and other forms of cyber-attacks. Through this survey, the study aims to gauge the extent of college students' awareness regarding these security threats and propose recommendations to address and mitigate these issues effectively.

Moveover, AlMindeel & Martins (2021) delved into the intricacies of employee information security awareness in the government sector, with a specific focus on the challenges encountered by public sector entities in developing nations during the implementation of information security awareness initiatives. Employing an interpretive research design, the study delves into perceptions, obstacles, aspirations, and facilitating factors related to information security awareness within the Saudi Arabian context. Through a single-case study methodology involving face-to-face interviews with senior personnel and document analysis, the research unveils the critical importance of individual awareness, knowledge, and behavior regarding information security, while also identifying key facilitators such as tailored approaches to employee and organizational needs, interactive methods, innovative strategies, consistent reinforcement, integration of electronic and physical resources, and incentivizing the acquisition of actionable security knowledge. By shedding light on these previously unexplored aspects, this study significantly contributes to the understanding of socio-technical dynamics surrounding information security awareness in government organizations in developing countries, particularly in Saudi Arabia, thereby enriching the existing literature in this domain.

7. Research Gap

1. **Nepalese Contextualization**: Limited exploration of Nepal's higher education sector, hindering understanding of local influences on cybersecurity awareness.

2. **Faculty and Staff Inclusion**: Neglect of faculty and staff perspectives, crucial for a holistic approach to cybersecurity in higher education.

3. **Longitudinal Studies**: Scarce longitudinal insights into the dynamic nature of cyber security awareness, essential for tracking evolution and assessing long-term effectiveness.

4. **Effectiveness of Interventions**: Lack of comprehensive assessments of awareness program effectiveness, hindering evidence-based initiative design in diverse educational settings.

8. Methodology

In this research, conducted within a private tertiary education institution in Kathmandu, Nepal, the research framework adopted a quantitative approach to examine cybersecurity awareness among faculty, staff, and students across three campuses. A total of 401 paper-based responses were collected from participants, and SPSS software was utilized for data analysis. The statistical techniques employed included descriptive statistics to provide an overview of the data, Pearson correlation analysis to explore relationships between variables, chi-square tests to examine associations between categorical variables, and Cronbach's alpha to assess the internal consistency reliability of the survey instrument (Douha et al., 2023). Through this comprehensive analytical approach, the study aimed to gain insights into the levels of cybersecurity awareness within the institution and identify potential areas for improvement in awareness programs and policies.

The questionnaire comprised six sections, delineated as follows:

i. Demographic information of the students

ii. Online usage patterns of the students

iii. Cybersecurity knowledge assessment

iv. Evaluation of students' self-perceived cybersecurity skills

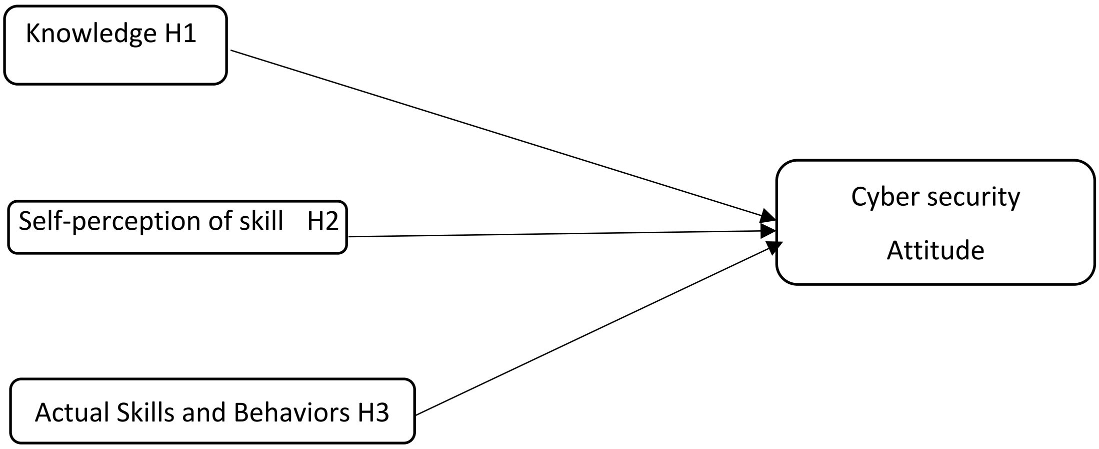
v. Examination of students' actual cybersecurity skills and behaviors

vi. Exploration of students' attitudes towards cybersecurity

TPB Framework Implement

The study utilized an adapted version of the Theory of Planned Behavior (TPB) framework, originally proposed by Icek Ajzen, due to its established relevance in exploring ethical behavior and compliance with computer security measures (Ajzen, 1991). While the TPB framework has been extensively used in such contexts, its direct application to C.A (CSA) required adaptation. Previous research on CSA was reviewed to identify essential variables and potential relationships, serving as a foundation for this study (Chandarman & Niekerk, 2017). Studies emphasized the critical role of CSA training and education in providing clarity and direction on security policies and practices (Wilson & Hash, 2022).

(Zwilling et al., 2022)It suggests that assessing CSA requires considering various factors such as attitudes, behaviors, self-perception of skills, and actual skills, as knowledge alone may not ensure CSA effectively. Accordingly, our adapted version of the TPB framework investigated CSA via focus on relationships among four core variables:



Conceptual Framework for Cyber security awareness

Hypothesis

Hypothesis (H1): There is a significant relationship between cyber security attitude and cyber security knowledge.

Hypothesis (H2): There is a significant relationship between cyber security attitude and self-perceptions of skills.

Hypothesis (H3): There is a significant relationship between cyber security attitude and actual cyber security skills.

Source of data

The study drew data from three reputable higher education institutions in the Kathmandu Valley, Nepal, chosen for their academic diversity and geographical spread. Through purposive sampling, participants representing various academic disciplines and demographics will be selected from each institution to offer a comprehensive perspective on cybersecurity awareness. This inclusive approach, encompassing both students and staff, aims to provide a nuanced understanding of C.A practices and perceptions within Nepal's higher education community, contributing to a broader comprehension of its implications for the region.

Data collection / Acquiring

Structured questionnaires were personally administered by the researcher to gather data on C.A, knowledge, attitudes, and behaviors. Direct interaction ensured clarity and consistency, with immediate clarification of doubts. Attention was given to ensure comprehensive responses, addressing any missing or unclear information promptly. Thorough review and verification ensured data completeness and accuracy, enhancing authenticity and reliability. This method facilitated a detailed understanding of participants' perceptions and experiences regarding C.A, contributing to robust research outcomes.

Instrument used

A structured questionnaire, meticulously designed based on existing literature and theories like the Theory of Planned Behavior, was the primary tool for data collection. It underwent rigorous validation by cybersecurity professionals and academic advisors. The questionnaire covered various aspects of C.A, including demographics, online usage, knowledge, skills, behaviors, and attitudes. Closed-ended questions predominated, offering standardized responses, while open-ended questions provided qualitative insights. Pilot testing ensured clarity and appropriateness. Overall, the questionnaire emerged as a robust instrument, facilitating comprehensive data collection and analysis aligned with research objectives.

Execution of the experiment

During the execution phase, thorough planning and systematic procedures were employed to implement the research methodology smoothly. This included securing ethical approval, recruiting participants through purposive sampling, and training research assistants. Data collection was conducted in controlled environments, with quality assurance measures in place. Post-collection involved validation and preprocessing of data. Adherence to rigorous standards and ethical guidelines ensured the validity of research findings, enhancing understanding of cyber security awareness in higher education institutions in the Kathmandu Valley.

Data analysis

Quantitative data from questionnaires will be analysed using SPSS, employing descriptive statistics for demographics and survey responses. Correlation and regression analyses will explore variable relationships and test study hypotheses. Qualitative data from interviews will undergo thematic analysis to identify patterns. Overall, the research design integrates quantitative and qualitative approaches to provide comprehensive insights into C.A among H.E stakeholders in Nepal.

9. Data Analysis

Table 1
Reliability Testing

Reliability Statistics

Cronbach's Alpha	N of Items
.726	25

The Cronbach's Alpha coefficient for the 25-item scale is .726, indicating moderate internal consistency reliability. Although slightly below the typical threshold of 0.7, it still suggests reasonable consistency in measuring the intended construct. Context, scale size, and research goals should be considered when interpreting Alpha values; further analysis may be warranted despite the acceptable level for many purposes.

The table 2 shows gender distribution among respondents using three metrics: percent, valid percent, and cumulative percent. Males make up 59.9%, females 40.1%. Valid percent adjusts for missing or invalid data, with both genders totaling 100%. Cumulative percent indicates the proportion of respondents up to each category. Overall, males constitute the majority at 59.9%, while females represent 40.1%.

Table 2 4.2
Frequency test for gender

Q.1 What is you gender ?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Male	240	59.9	59.9	59.9
	Female	161	40.1	40.1	100.0
	Total	401	100.0	100.0	

Inferential Analysis

Table 3

Correlation

Correlations

		Attitude	Knowledge	ActualSkill	Selfperception skill
Attitude	Pearson Correlation	1	.335	.322	.434
	Sig. (2-tailed)		.000	.000	.000
	N	401	401	401	401

Knowledge	Pearson Correlation	.335	1	.512	.318
	Sig. (2-tailed)	.000		.000	.000
	N	401	401	401	401
ActualSkill	Pearson Correlation	.322	.512	1	.400
	Sig. (2-tailed)	.000	.000		.000
	N	401	401	401	401
Selfperceptionskill	Pearson Correlation	.434	.318	.400	1
	Sig. (2-tailed)	.000	.000	.000	
	N	401	401	401	401

Correlation is significant at the 0.01 level (2-tailed).

The table 3 presents correlations between four variables: Attitude, Knowledge, Actual Skill, and Self-Perception Skill. Positive correlations were found between Attitude and Knowledge (r = 0.335, p < 0.01), Attitude and Actual Skill (r = 0.322, p < 0.01), and Attitude and Self-Perception Skill (r = 0.434, p < 0.01), indicating that a positive attitude towards cybersecurity is associated with higher levels of knowledge, actual skill, and self-perceived skill in this domain. Moreover, Knowledge and Actual Skill exhibited a strong positive correlation (r = 0.512, p < 0.01), suggesting that greater knowledge about cybersecurity is linked to higher levels of actual skill. Additionally, a significant positive correlation was observed between Actual Skill and Self-Perception Skill (r = 0.400, p < 0.01), implying that individuals who demonstrate higher levels of actual skill tend to perceive themselves as more skilled in cybersecurity. These findings underscore the interconnectedness between attitudes, knowledge, and kills related to cybersecurity, highlighting the importance of fostering positive attitudes and enhancing knowledge to improve skills in this domain.

Table 4

Regression analysis

Model Summary[b]

					Change Statistics				
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	R Square Change	F Change	df1	df2	Sig. F Change
1	.488[a]	.238	.232	.49376	.238	41.300	3	397	.000

a. Predictors: (Constant), Self- perception skill, Knowledge, Actual Skill

b. Dependent Variable: Attitude

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	30.207	3	10.069	41.300	.000[b]
	Residual	96.789	397	.244		
	Total	126.996	400			

a. Dependent Variable: Attitude

b. Predictors: (Constant), Self-perception skill, Knowledge, Actual Skill

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients		
		B	Std. Error	Beta	t	Sig.
1	(Constant)	1.957	.228		8.595	.000
	Knowledge	.155	.045	.178	3.463	.001
	Actual Skill	.089	.050	.095	1.788	.074
	Self-perception skill	.315	.045	.339	7.025	.000

a. Dependent Variable: Attitude

The regression model exhibits an R Square value of 0.232, indicating that approximately 23.2% of the variance in attitudes towards cybersecurity can be explained by the predictor variables. The F Change statistic is significant (p < 0.001), suggesting that the addition of the predictor variables significantly improves the model's explanatory power.

The ANOVA table indicates that the regression model is statistically significant (F = 41.300, p < 0.001), suggesting that at least one of the predictor variables significantly predicts attitudes towards cybersecurity.

The coefficients table shows the unstandardized coefficients (B) and standardized coefficients (Beta) for each predictor variable. Self-Perception Skill emerges as the most influential predictor, with a significant positive relationship with Attitude (B = 0.315, p < 0.001). Knowledge also shows a significant positive relationship with Attitude (B = 0.155, p = 0.001), while the relationship between Actual Skill and Attitude is marginally significant (B = 0.089, p = 0.074).

Overall, these findings suggest that self-perceived skill in cybersecurity, followed by knowledge about cybersecurity, significantly influence attitudes towards cybersecurity. However, the relationship between actual skill and attitudes is less pronounced and warrants further investigation.

10. Conclusion

The analysis supports the hypotheses that cyber security attitude is positively related to both cyber security knowledge and self-perceptions of skills. However, the relationship between cyber security attitude and actual cyber security skills requires further investigation due to the marginally significant p-value.

11. Recommendations

Emphasize Cyber Security Education: Given the significant positive relationship between cyber security attitude and cyber security knowledge, educational institutions and organizations should prioritize initiatives aimed at enhancing cyber security awareness and knowledge among individuals. This could involve integrating cyber security education into academic curricula and offering training programs for students, faculty, and staff.

Foster Self-Perception of Skills: Since self-perceived skills in cyber security significantly influence attitudes towards cyber security, efforts should be made to empower individuals to develop confidence in their cyber security skills. Providing opportunities for hands-on practice, offering mentorship programs, and recognizing achievements in cyber security can help bolster individuals' confidence in their abilities.

Strengthen Practical Skill Development: Although the relationship between cyber security attitude and actual cyber security skills is inconclusive, there is potential for improvement in this area. Institutions and organizations should focus on implementing practical skill development initiatives, such as hands-on training workshops, simulations, and real-world projects, to bridge the gap between perceived and actual cyber security skills.

References

Ajzen, I. (1991). The theory of planned behavior. Organizational Behavior and Human Decision Processes, 50(2), 179–211. https://doi.org/10.1016/0749-5978(91)90020-T

AlMindeel, R., & Martins, J. T. (2021). Information security awareness in a developing country context: insights from the government sector in Saudi Arabia. Information Technology and People, 34(2), 770–788. https://doi.org/10.1108/ITP-06-2019-0269

Alqahtani, M. A. (2022). Factors Affecting Cybersecurity Awareness among University Students. Applied Sciences (Switzerland), 12(5). https://doi.org/10.3390/app12052589

Chandarman, R., & Niekerk, B. Van. (2017). Students ' Cybersecurity Awareness at a Private Tertiary Educational. The African Journal of Information and Communication (AJIC), 20, 133–155.

Douha, N. Y. R., Renaud, K., Taenaka, Y., & Kadobayashi, Y. (2023). Smart home cybersecurity awareness and behavioral incentives. Information and Computer Security, 31(5), 545–575. https://doi.org/10.1108/ICS-03-2023-0032

Ikhalia, E., Serrano, A., Bell, D., & Louvieris, P. (2019). Online social network security awareness: mass interpersonal persuasion using a Facebook app. Information Technology and People, 32(5), 1276–1300. https://doi.org/10.1108/ITP-06-2018-0278

Maharjan, R., & Chatterjee, J. M. (2019). Framework for Minimizing Cyber Security Issues in Banking Sector of Nepal. LBEF Research Journal of Science, 1(1), 82–98.

Rawindaran, N. (2023). Impact of cyber security awareness in small, medium enterprises (SMEs) in Wales. /articles/thesis/Impact_of_cyber_security_awareness_in_small_medium_enterprises_SMEs_in_Wales/23599497/1

Senthilkumar, K., & Easwaramoorthy, S. (2017). A Survey on Cyber Security awareness among college students in Tamil Nadu. IOP Conference Series: Materials Science and Engineering, 263(4). https://doi.org/10.1088/1757-899X/263/4/042043

Wilson, M., & Hash, J. (2022). Nist Sp 800-50. Nist, October, 70.

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber Security Awareness, Knowledge and Behavior: A Comparative Study. Journal of Computer Information Systems, 62(1), 82–97. https://doi.org/10.1080/08874417.2020.1712269