NIJEC 5 (1) (2026) 1-14

NUML International Journal of Engineering and Computing

Journal Homepage: NIJEC.NUML.edu.pk

Print ISSN: 2788-9629

Cybersecurity Awareness and Preparedness of Academic Library Professionals in Pakistan: Bridging the Training Gap in Digital Libraries

Sahar Afshan[a]*, Maryam Naveed[a], Hassan Shah Khan[a], Sobia Ayaz[a]

[a] Faculty Of Engineering, Sciences, Technology & Management Library, Ziauddin University, Karachi, Pakistan

ARTICLE INFO

Article History:
Received 20
Accepted 025
Available Online 6

Keywords:
Cybersecurity Awareness; Academic Libraries; Library Professionals Pakistan; Cybersecurity Awareness Paradigm; Professional Development; Information Security; Digital Libraries

Funding:
This research received no specific grant from any agency in public, commercial or non-for-profit sector

Conflict of Interest:
The author has declared no potential conflicts of interest and falsification/fabrication of data with respect to the research, authorship, and/or publication of this article.

ABSTRACT

The digitization trend of academic libraries along with increased vulnerability to cyber security threats is discussed in the present research, in order to conduct quantitative analysis of cyber security issues in the context of academic library professionals in Pakistan, 101 participants have been surveyed using basic statistical analysis techniques. These findings suggest high levels of involvement in protection activities (M = 3.90) and good awareness of cybersecurity issues (M = 3.55). Hence, the respondents believe themselves capable of implementing protective actions even without regular training courses in this domain. However, despite positive perceptions about institutional support (M = 4.06), low frequency of cybersecurity training sessions (M = 2.98) points to a significant discrepancy between individual skills and organization readiness to deal with emerging risks. In addition, the study participants have increasingly grown worried by the growing role played by AI technologies in the operation of libraries as well as by new types of cyberattacks. This paper explores the ways in which academic libraries in developing countries react to such fast-developing risk factors. The paper takes a socio-technical approach that covers individuals' awareness of cybersecurity problems, their security-related actions performed in working and non-working settings, and institutional management of security.

1. Introduction

1.1. *Digital Transformation and the Expanding Cybersecurity Role of Academic Librarians*

The rapid digitalization due to electronic resources and cloud computing, institutional repositories, AI etc., in academic libraries has literally opened up a vast ocean of information with easy access. But it has led to a greater risk of cybersecurity. [1][2]. While libraries exist in a continuum of transitions, academic library practitioners have shifted from being passive custodians of knowledge to become information managers of not only systems but also user data and ethical practices of information use [3][4], thus their cyber resilience is crucial for the sustenance and growth of their institutions. These vulnerabilities and high stress on librarians to build secure digital space [5] [6], is further complicated in less developed countries like Pakistan where low resources and unequal preparedness are prevalent. Academic librarians have shifted their attention to print

https://doi.org/10.52015/nijec.v5i1.118

*Corresponding Author: Sahar Afshan: sahar.afshan@zu.edu.pk

collection management to handling intricate digital and AI-driven information systems, making them a significant force in information protection and user privacy concerns [7]. Librarians, as the linking activity between users and information infrastructures, need not only technical skills but a high level of awareness of cybersecurity risks, ethical accountability, and data protection activities [8][9]. Consequently, universities are increasingly requiring librarians to assist in providing secure digital learning conditions, and thus, cybersecurity awareness is an essential professional skill [10].

1.2. *Cybersecurity Threats and Awareness Issues in Academic Libraries:*

Academic libraries are most likely to target cyberattacks because of their extensive digital assets, including databases, research outputs, institutional records, and user credentials, and their open-access policies.[11][12]. Phishing, ransomware, data breaches, and unauthorized access are also considered core threats that have been reported extensively with the growth of attack surfaces due to the growth of digital libraries and remote services. Artificial intelligence and cloud-based systems have improved library services, but they have also presented sophisticated cyber threats that most libraries are not currently prepared to deal with [13][14][15]. Empirical research studies reveal that academic librarians have medium to low levels of awareness of cybersecurity, particularly when it comes to advanced threats and safe practices in the digital environment, which is mainly shaped by access to training and organizational culture [16][17][18]. Such issues are particularly acute in developing environments like Pakistan, where digital adoption has exceeded cybersecurity capacity-building activities [19][20].

1.3. Research Trends, Empirical Gaps, and the Pakistani Context of Academic Library Cybersecurity

While international research increasingly emphasizes the human factor and awareness frameworks in library cybersecurity, most studies focus on students or developed regions, leaving gaps in understanding librarians' awareness, practices, and perceived challenges in developing countries [21][22][23][24][25]. Additionally, various conceptual and framework-based research present awareness models, which lack adequate empirical validation in academic library settings [26][27][28].It suggests that context-related and information-based studies should be conducted that consider the level of awareness and support mechanisms in institutions. Rapid adoption of digital and AI in academic libraries has significantly increased cybersecurity risks in Pakistan, whereas systemized evidence regarding the awareness of librarians, the effectiveness of policy, and institutional support is low [29][30]. The risks are further increased by weak security policies and low staff preparedness, and support the necessity of context-specific empirical research [31]. In light of these contextual issues, empirical evaluation of cybersecurity learning among academic library professionals in Pakistan is essential and timely.

1.4. Purpose and Significance of the Present Study

This study aims to explore cybersecurity awareness and preparedness of academic library professionals in Pakistan via a three-dimensional analysis of individual awareness, protective practices, and institutional support. The research will explore the interaction between human behavior, organizational, and technological environment, and their influence on cybersecurity preparedness in academic libraries through a socio-technical approach. Particularly, the research question that is being addressed is how much library professionals are aware of cybersecurity, practice in risky ways, and are sensitive to institutional activities that are intended to enhance cybersecurity resilience. The results will be used to enhance theoretical knowledge and practical policy-making processes through evidence-based knowledge that will help in the building of training programs, governance frameworks, and sustainable cybersecurity policies to academic libraries.

1.5. Research Questions

Q1. How educated in cybersecurity are Pakistani academic library professionals?

Q2. How do librarians see cybersecurity, perceived risk, and individual accountability?

Q3. What risks related to cybersecurity and policy gaps do academic library professionals observe in their institutions?

Q4. What organizational assistance can be provided to enhance cybersecurity readiness, and what are the recognized training requirements?

2. Literature Review

Academic libraries' rapid digital transformation has increased information accessibility while increasing cybersecurity issues. Instead of focused only on technological restrictions, current literature describes cybersecurity as a socio-technical issue influenced by technology, human behavior, and institutional governance. A comparative study of significant studies and research gaps pertaining to academic library professionals' understanding of cybersecurity is presented in Table 1.

Table 1 Comparative Analysis of Existing Studies on Cybersecurity Awareness in Academic Libraries

Year	Author(s)	Study Type	Focus Area	Research Gap
2001	A. Goetsch	Case study	Security culture in university libraries	Lacks empirical data on librarian awareness
2012	S. K. W. Fakeh et al.	Empirical study	Information security awareness	Limited by a small sample and no framework
2014	K. Arlitsch & A. Edelman	Review	Cybersecurity for organizations	Not library-specific; lack of structured programs
2018	N. Tummon & D. McKinnon	National survey	Librarians' privacy attitudes	Training effectiveness is not examined
2019	I. Ajie	Review	Cybersecurity trends in libraries	No empirical assessment of librarians
2023	A. Aregbesola & E. L. Nwaolise	Best practices review	Securing digital collections	No evaluation of librarian awareness
2023	O. Adenike & R. Alabi	Survey	Librarians' awareness & perception	No structured improvement framework
2023	M. O. Igbinovia & B. C. Ishola	Empirical study	Cybersecurity in Nigerian libraries	Training interventions absent
2023	A. M. Alhaif	Survey	Training needs of library staff	Program effectiveness untested
2024	K.-R. Kont	Survey	Library employees' security awareness	No tested interventions
2024	K. R. Kont	Review	Human factor in cybersecurity	No quantitative staff assessment
2024	S. Panda & N. Kaur	Book chapter	Cybersecurity awareness of librarians	No measurable outcomes or framework
2025	I. Magsi et al.	Survey	Digital library cybersecurity challenges	Intervention studies missing
2025	R. Armas & H. Taherdoost	Conceptual	Cybersecurity culture in higher education	Needs practical validation
2025	E. Pasipamire	Systematic review	Awareness frameworks & best practices	Practical effectiveness untested
2025	M. Y. Ali	Survey	Cybersecurity threats in Pakistani libraries	No structured awareness programs
2025	K. Komane et al.	Conceptual framework	Cybersecurity awareness framework	Needs empirical validation
2025	M. F. Baharuddin et al.	Survey	Digital literacy & cybersecurity	Librarian-focused training missing

2.1. Early Research [2001]: Security Culture and Institutional Responsibility

Early research determined training employees, institutional responsibility, and security culture as the fundamental elements of cybersecurity awareness [3]. Although further studies addressed contextual differences, early research emphasized organizational dedication over technical security. As libraries in developing countries experienced difficulties because of limited resources, inadequate management, and policy gaps, advanced institutions demonstrated organized cybersecurity training This indicates that earlier models did not have enough real-world evidence when resources were limited and they failed to recognize existing unfair advantages in society.

2.2. Human Factors and Awareness (2012–2014)

The focus shifted to human-factor weaknesses, privacy awareness, and policy clarity [12][16]. Some studies show that moderate cybersecurity levels among library professionals do not lead to secure behavior unless there are strong institutional policies, regular training, and active support from supervisors. Established institutions have well-organized structures but are often under-resourced. In contrast, new settings have disconnected governance structures, and gaps between knowledge and practice exist.

2.3. Policies and Training Programs (2016–2019)

Between 2016 and 2019, written policies and systematic training were recommended as threat response strategies.[1] [8][19]. Cybersecurity awareness can be raised through training, yet sustained, context-specific programs supported by management are required to sustain long-lasting behavioral changes. There is a lack of policies; compliance needs to be actively enforced and institutionalized.

2.4. Behavioral and Organizational Perspectives (2020–2022)

In the recent studies regarding this period, the psychological and organizational orientations were included in the field of cybersecurity studies. [6][20][30]. Even though the awareness of library professionals became better, the compliance with recommended practices was not even. Leadership, culture, and supervision were the important factors, which demonstrated that knowledge is not sufficient and successful cybersecurity requires active enforcement and effective organizational governance.

2.5. Recent Studies (2023–2025): AI, Evolving Threats, and Governance

Recent research discusses the impact of the evolving digital threats, governance of issues, and artificial intelligence on cybersecurity preparedness [2][5-6]. Phishing, ransomware, insider attacks, and unauthorized access attacks are typical threats [20][29][32]. The contextual changes also play an important role: Pakistan has no training and increased vulnerabilities regarding AI [36][38]; Turkiye has excessive institutionalization and Nigeria and Saudi Arabia lack infrastructure and are unprepared to employees [18][21][33]. Institutions which are richly endowed are concerned with coordination and interdepartmental integration [34][20]. All these studies indicate that the success of cybersecurity is more about the institutional capacity, governance, and strategic oversight than technology. Although AI results in improved threat detection, it has created new vulnerabilities to ethical and cyber security [22[27][38], and human factor vulnerabilities are still present despite the technological advancement [18][32][33] [39][40].

2.6. Training, Policy, and Leadership

Factors such as training, implementation of policies, and involvement of leaders have made organizations better prepared in terms of cybersecurity [5-7][8][11]. Nonetheless, the enforcement of regulations in many cases is lacking, especially when organizations face resource constraints [19][20][24]. The above points highlight the fact that cybersecurity is essentially a matter of governance and not just technology. For building up a strong security culture, proper implementation, training of people, and governance are necessary.

2.7. Research Gap

Current research on cybersecurity preparedness among academic libraries is highly scattered and inadequately incorporates the framework of Cybersecurity Awareness Paradigm, with no comparative studies between institutions for greater generalization This paper closes these gaps by incorporating the consciousness, behavior, training, and institutional element into a single context with evidence-specific to the context of Pakistan, where the librarian in the developing world is still under-researched [6][19][31]. The research that is already there including studies from Pakistan, Nigeria and other places shows that there are problems with people knowing about things with the infrastructure with training and with putting policies into action [13][20][22][24][30][34]. The thing is, these studies look at each of these issues on their own. The old models were more about how organizations work and not so much about technology but they assumed that the institutions were ready which is not always the case. This is especially true in developing countries where

resources and policies are limited. This is a big part of the problem with fairness in different contexts. Research on Pakistan, Nigeria and other settings shows that these issues are all connected, to the problem of resource and policy limits and that is what is really affecting Pakistan, Nigeria and other settings.

2.8. Conceptual Framework for the Present Study

The present study requires to fill this gap by incorporating the Cybersecurity Awareness Paradigm [32][33] which proposes that the awareness is a multidimensional construct, which is influenced by knowledge, attitudes and behaviors and is determined by organizational culture, training, policies and managerial support. This framework helps to explore the individual and institutional factors of cybersecurity preparedness in Pakistani academic libraries in detail. According to the Cybersecurity Awareness Paradigm, cybersecurity readiness is defined as a relationship among awareness, attitude, behavior, and institutional culture, such that awareness coupled with good attitudes leads to safe behavior in the presence of institution-based training and management support.

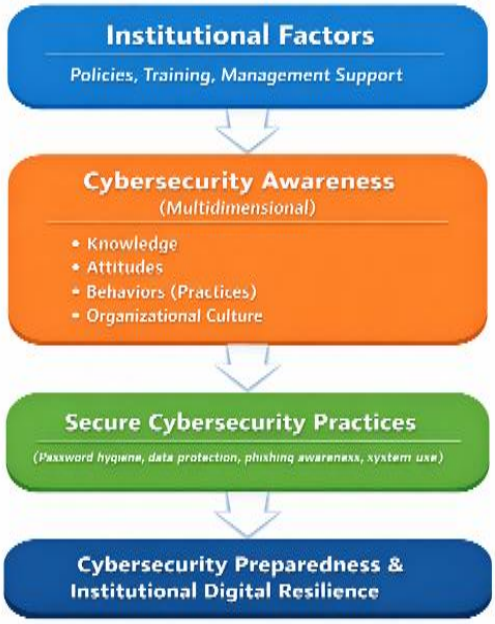

Figure 1. Cybersecurity awareness paradigm linking institutional factors, awareness dimensions, secure practices, and overall preparedness.

3. Methodology

3.1. Research Design:

The research was conducted using a quantitative cross-sectional survey method to examine the level of cyber security awareness, behavior, and institutional preparedness among librarians working in academic libraries in Pakistan. The approach used in this research takes into account a socio-technological approach in assessing the correlation between awareness, organization, and behavior.

3.2. Population and Sampling

The survey focused on professional academic librarians working in public and private higher the study targeted academic library professionals working in higher education institutions across Pakistan. Due to there exists no comprehensive national sampling frame and variations in institutional accessibility, purposive sampling was employed to recruit participants with relevant professional experience in digital library environments. This

approach enabled the inclusion of information professionals directly engaged in cybersecurity-related practices, providing contextually informed insights despite limited statistical generalizability.

It is important to note that the overall sample size of this research was 101 professional librarians working in academic libraries, which is suitable to conduct exploratory social science research and similar to other studies on cybersecurity awareness that employed purposive sampling, with a sample size ranging between 85 and 115 respondents.[4][6][20][26]. Although non-probability sampling methods limit the study's generalizability due to the small number of respondents, purposive sampling allowed for informed participation by the targeted respondents.

The following was the demographic structure of the sample.

i. Gender distribution: 53% males (n=54) and 47% females (n=48), the numbers of both sexes are equally represented.

ii. A significant number, 80% of responders, were assistant librarians (40.6%, n=41) and librarians (38.6%, n=39). The remaining ones were deputy librarians and chief librarians.

iii. Experience in profession: The largest number of participants (71.3%, n=72) had less than ten years of experience in their professions.

iv. Affiliation of organization: 68.3% (n=69) of the respondents were employed in private organization and the remaining 31.7% (n=32) in government universities.

v. Qualifications of participants: They were all qualified in Library and Information science (LIS).

vi. Computer skills: Majority of them were moderate-high computer users.

3.3. Survey Instrument:

A structured, self-reported questionnaire was administered to gather the data and included three parts with a five-point Likert scale (1 = Strongly Disagree to 5 = Strongly Agree)

The questionnaire comprised three sections:

i. Section A: Cybersecurity awareness and knowledge

ii. Section B: Cybersecurity practices

iii. Section C: Training, attitudes, and institutional support

3.4. Instrument Validity and Reliability

i. Cybersecurity Awareness: $\alpha = 0.81$

ii. Cybersecurity Practices: $\alpha = 0.79$

iii. Training/Support: $\alpha\alpha = 0.88$

The questionnaire was reviewed for clarity and relevance through expert evaluation to ensure alignment with study objectives and theoretical constructs.

3.5. Data Collection and Analysis:

i. The survey was distributed off electronically to academic library professionals, with voluntary participation and anonymous responses to promote honest reporting and minimize social desirability bias.

ii. The academic library professionals were given structured questionnaires. Python was used to analyze the data with Pandas, NumPy, SciPy, and Matplotlib.

iii. Descriptive statistics, which includes mean scores and standard deviations, were implemented to evaluate awareness, practices, and institutional preparedness. This method was appropriate for recognizing generalized preparedness trends and institutional deficiencies, consistent with the

study's exploratory emphasis on organizational evaluation rather than causal or predictive evaluation.

4. Survey Results and Analysis:

The analysis of data was performed in Python (Pandas, NumPy, SciPy and Matplotlib). Descriptive statistics (frequencies, percentages, means, and standard deviations) summarized the respondent characteristics and significant variables, and the independent samples t-tests were used to test the differences across variables, including gender, department, professional background, and computer skills level.

Figure 2 shows the roles and institutional distribution of respondents. Almost 80% of participants were comprised of Librarians and Assistant Librarians, and the vast majority of respondents had less than 10 years of professional experience. Most of the sample was represented by the private universities (68.3) meaning that there was a good representation of early-mid-career professionals, especially the ones in the private sector.

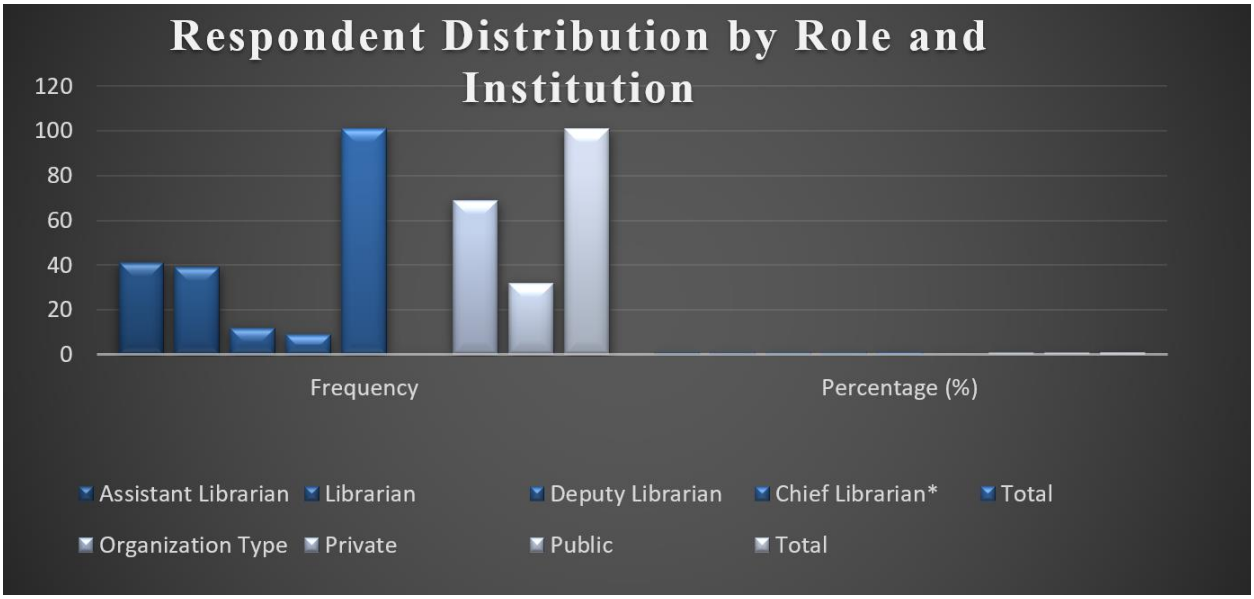

Figure 2. Distribution of Respondents by Professional Role and Institutional Type (Frequency and Percent

Figure 3 showed that the proportion of public librarians in the awareness level category (65.6) was more than that of the private librarians (50.7). The percentage of moderate and low are relatively higher in private librarians, and both categories have similar proportions in the very high awareness level. On the whole, the level of cybersecurity awareness is relatively higher among the public librarians.

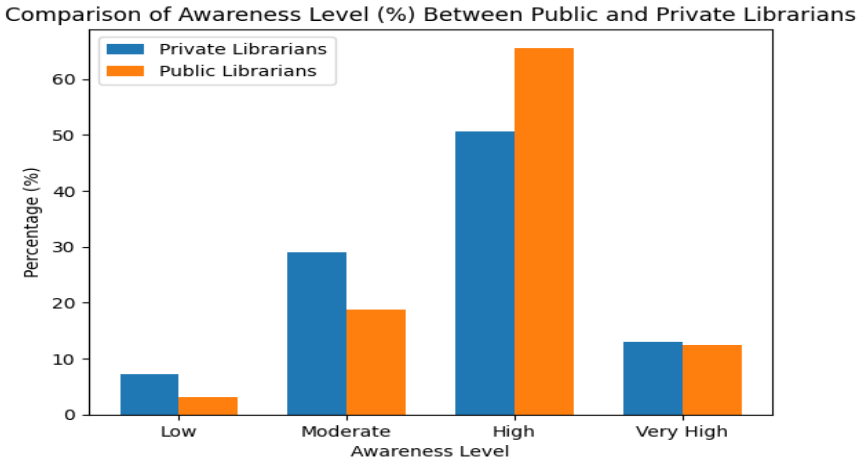

Figure 3. Comparison of Cybersecurity Awareness Levels Between Public and Private Librarians

4.1 Cybersecurity Awareness & Knowledge (N=101).

The mean of awareness (M = 3.55, SD = 0.92) is average, which is consistent with Farid et al. [19] and Panda and Kaur [31] in South Asia. Being less than Kavak [26] in Turkiye probably because of more powerful policies and compulsory training, it is higher than Ali [34] in Pakistan, indicating that awareness is determined by institutional capacity, policy implementation, and access to organized training in developing setting.

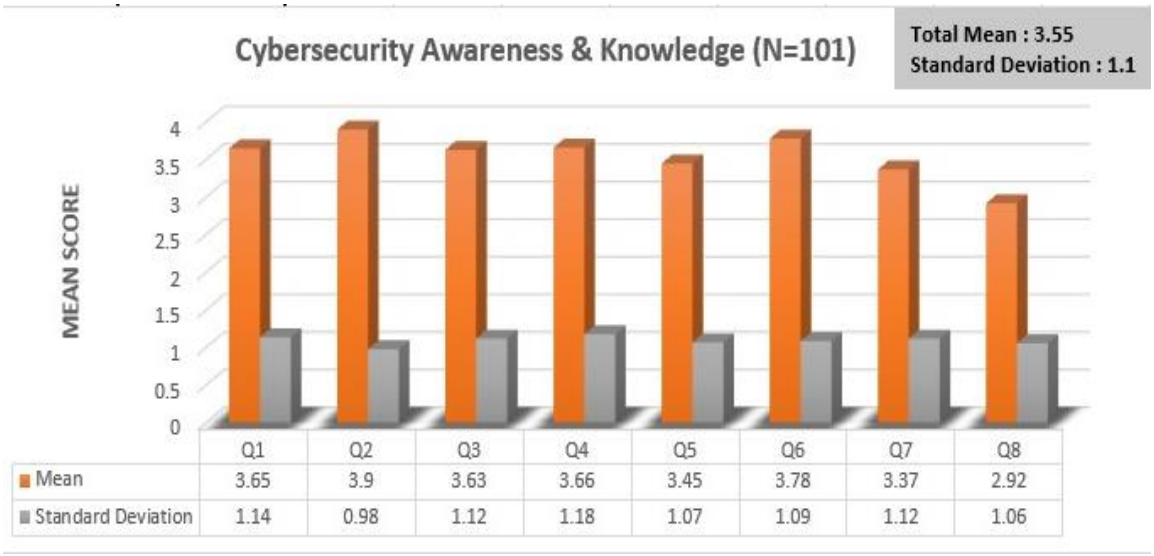

Figure 4. Cybersecurity Awareness Levels Across Survey Questions (Q1–Q8)

4.2 Cybersecurity Practices (N=101)

The means of academic library professionals demonstrated high levels of cybersecurity practices (M = 3.90, SD = 1.00) with the items means of 3.57-4.14, and consistent use of safe daily practices even in the conditions of moderate awareness and low advanced skills. This affirms the Cybersecurity Awareness Paradigm and the previous findings that awareness results in safe behavior but gaps in training still exist to show that awareness cannot be sustained as a lasting method of assuring long term preparedness without strong institutional support.

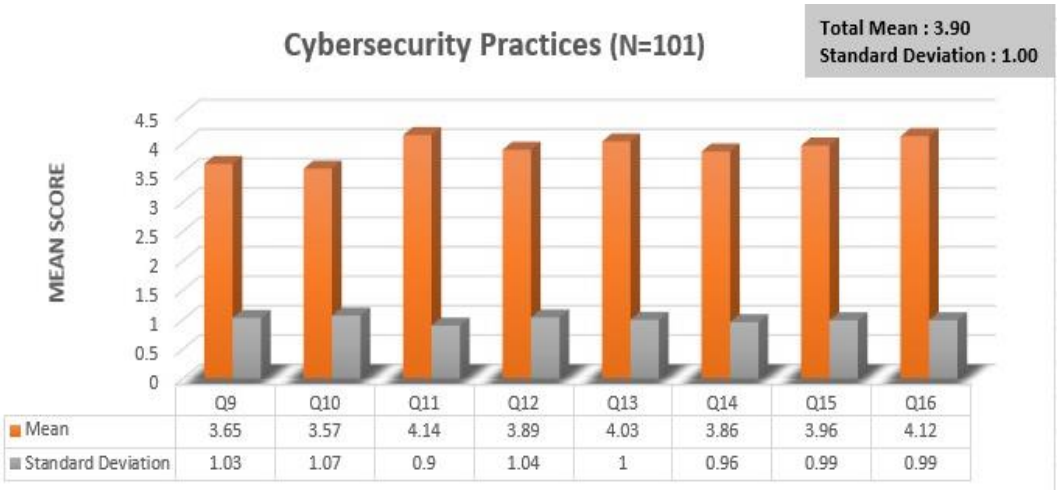

Figure 5. Cybersecurity Practice Across Survey Questions (Q9–Q16)

4.3 Training, Attitude & Institutional Support (N=101)

The respondents expressed excellent attitudes regarding cybersecurity and indicated high levels of perceived institutional support (M = 4.06, SD = 0.94) where majority of the measures are over 4.0. However, formal training was quite low (M = 2.98, SD = 1.21), which is the primary gap: supportive organizational conditions do not necessarily mean that there is a systematized capacity-building, and the institutional policy limitations are the issue, not failures of individuals.

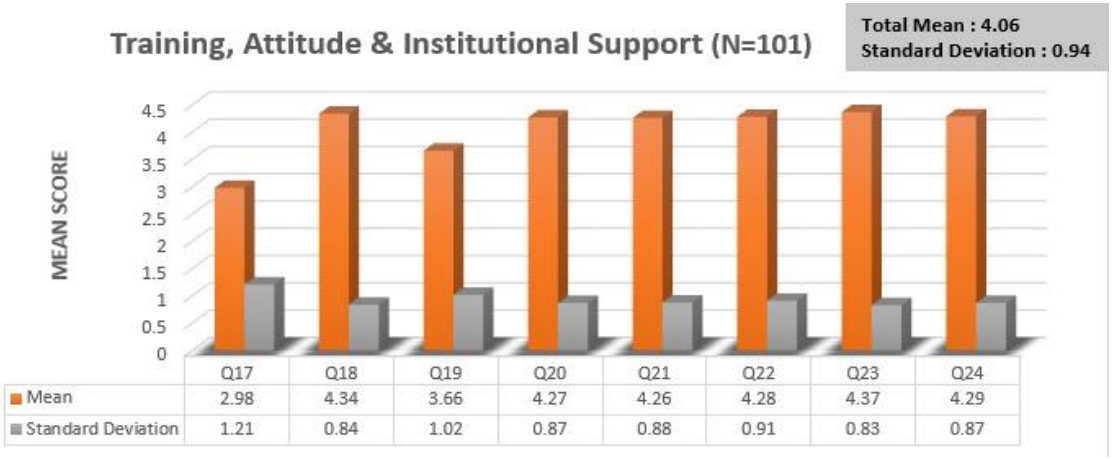

Figure 6. Cybersecurity Training, Attitude and Institutional Support Across Survey Questions (Q17–Q24)

4.4 Comprehensive Overview of Mean Scores

Figure 7 shows the line graph for the mean scores on cybersecurity awareness in Q1 to Q24. The vast majority of the questions scored between 3.4 and 4.2, with Q17 scoring about 2.9. On the other hand, questions Q11, Q18, and Q20-Q24 score between 4.3 and 4.4. The scores match those discussed in previous works as being problems that needed attention. As a matter of fact, the trends observed in the study follow previous evidence and literature. It has been seen in previous studies that libraries have high cybersecurity awareness but that more training and policy implementation were required. (Farid et al., 2023; Panda and Kaur, 2024).

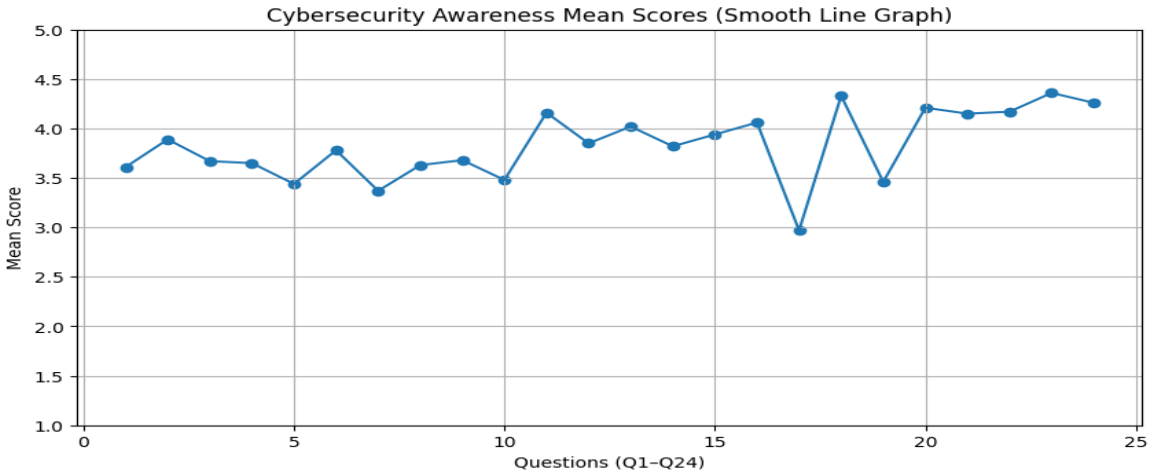

Figure 7. Cybersecurity Awareness Mean Scores Across Survey Questions (Q1–Q24)

5. Ethical Considerations:

Ethical standards were followed closely: people joined voluntarily, they knew what they were signing up for they were assured that their answers would be maintained as private and confidential. No personal information was collected, and anyone could decide to leave at any moment.

6. Results and Discussion:

This section, based on the Cybersecurity Awareness Paradigm, discusses about how awareness, practices, attitudes, and institutional factors all work together to impact how well-equipped academic library professionals in Pakistan are to deal with cybersecurity. We compare the results of our study to individuals of earlier studies to determine where they correspond and where they disagree.

6.1 Cybersecurity Awareness, Practices, and Perceived Threats Among Respondents (Q1, Q2, Q3)

The results indicate that the level of cybersecurity awareness among academic library specialists is generally favorable and most of the respondents demonstrated that they were sufficiently informed about online dangers and preventive actions.[8][11].Nevertheless, institutional preparedness is found to be relatively less, implying that personal awareness is not well-guaranteed by the organized organizational processes. This conclusion supports the view of cybersecurity as a socio-technical issue that is fueled by governance and institutional capacity and not by technical knowledge.[20][24].

6.2 Training Requirement and Organizational Support (Q4)

Formal cybersecurity training (M = 2.98) was not accessible and the institutional support was high (M = 4.06) showing a gap in implementation. Attitudes and knowledge were found to promote safe practices positively but lack of training influences the long-term preparedness. This is a tendency, typical of the libraries of the developing countries, showing that no policy and encouragement can substitute constant training and involvement of active leaders [20][24][34].

6.3 Explaining Contradictions with Prior Literature.

i. High practices vs. low training: Contrary to the well-resourced environment (Kont, 2023; Kavak, 2024), where high training predicts secure behavior, in Pakistan, high-practice adoption is observed in the absence of formal training, likely due to informal learning, and focus on basic protective behavior.

ii. Public vs. private awareness there is an increased level of awareness in public sector librarians (65.6) compared to their counterparts in the private sector (50.7%), which indicates that regulation and stability in the institution can be more important than access to resources.

iii. Perceived support vs. actual training: High perceived support (M = 4.06) relates to low training (M = 2.98) meaning that perceived support is more of an overall climate of the organization than resources [19-20].

7. Limitations of the Study:

This study has several methodological limitations:

i. Small sample size (n = 101)

ii. Non-probability purposive sampling, which may introduce selection bias and limits generalizability

iii. Self-reported data, which may be subject to response bias.

iv. Limited advanced statistical analysis, restricting deeper causal interpretation.

Purposive sampling, small sample size, self-reported data and cross-sectional design are weaknesses in the study limiting the generalizability and causal interpretation. The nature of the research is exploratory due to basic statistical tests employed, but also provides the basis of evidence to future large-scale research.

8. Conclusion:

The current research, knowledge about cybersecurity, behaviors related to cyber practice, and perceived organizational support regarding cybersecurity of 101 library staff members working in academic libraries in Pakistan was analyzed, and it was found that there exists moderate knowledge of cybersecurity (M = 3.55) and high-level engagement in cybersecurity practices (M = 3.90) among them. Even if individuals have a positive attitude towards cybersecurity as well as their organization's attitude towards supporting cybersecurity (M = 4.06), lack of proper training (M = 2.98) highlights the gap between individual competence and organizational capability. Considering the Cybersecurity Awareness Paradigm, the findings of the current research indicate that cybersecurity is dependent on competent individuals, organizational policies, competent leadership, and continuous training sessions. Furthermore, it can be understood from the findings of this study that differences exist in the case of organizations which adopt an open cybersecurity policy compared to those organizations that do not have such a policy. These insights can be reinforced and used to inform evidence-based policies and training by future studies that have larger and representative samples and more sophisticated approaches. In sum, the research shows that academic library cybersecurity preparedness is contingent on both individual and institutional awareness, in particular, in the framework of developing countries.

9. Future Recommendations:

9.1 Refine Training Content and Delivery:

Training of librarians on the topic of cybersecurity should not be confined to the premises of knowledge only; it should be expanded to include sophisticated technical skills and emerging technologies. It should address sophisticated attacks such as zero-day attacks and APTs as it develops viable skills in the shape of simulations and actual attacks. The training content should be job role-specific and be supported by lifelong learning to ensure that it is constantly updated regarding the emerging cybersecurity threats and practices.

9.2 Strengthen Institutional Policies:

The libraries must develop cybersecurity policies that are user-friendly on issues pertaining to acceptable use, data handling, reporting of incidents, and remote access. Responsibility must be given out in terms of position in staff. Institutions should have specific resources to train systematically and improve their infrastructure, and have security tools. Review of policies to respond to the evolving threats and technology should be frequent, compliance checking and control mechanisms should be in place to build a compliance and accountability culture regarding cybersecurity.

9.3 Enhance Understanding of Organizational Culture:

Cultural aspects, perceptions, and other behavioral norms that determine cybersecurity practices should be explored using qualitative research designs (interviews and focus groups). These strategies will guide handy on building obstacles to quality training and implementation of policies such as time, shortage of skills and resistance to change. The availability of the library leadership and IT departments will also contribute to a more comprehensive perception of the institutional issues and the support systems to create certain and situation-specific cybersecurity interventions.

9.4 Promote Collaboration and Knowledge Sharing:

The institutions will be required to develop the minimum measurements to test and determine the extent of cybersecurity awareness, practices, and support systems. They also review it on a regular basis after some time so as to know the usefulness of the training and the policies. To improve the situation, a structured approach is required to analyze the input in terms of decreasing the incident and developing digital strength via feedback mechanisms. Furthermore, improved coordination across IT departments and libraries, as well as regional/national forums, will aid in the dissemination of best practices and a coordinated response to emerging risks.

9.5 Integration of Cybersecurity into LIS Curricula:

Cybersecurity modules should be introduced as a mandatory component of Library and Information Science (LIS) degree programs, and standardized curriculum instructions are being developed in collaboration with library and information science departments and professional organizations, such as digital information hygiene, detection of threats, and incident management, to address the gap in formal training and technical expertise among library practitioners in Pakistan.

9.6 Development of a National Cybersecurity Framework for Academic Libraries:

To bridge the gap between personal cybersecurity practices and institutional cybersecurity support, it is proposed that academic libraries in Pakistan establish a national cybersecurity framework to standardize security practices. This framework will be designed in consultation with academic libraries, IT departments, government agencies, and cybersecurity professionals.

Acknowledgment

I sincerely thank all the respondents for their time, cooperation, and valuable input, which made this study possible.

Author Contributions

Sahar Afshan (1st author): Formulating the idea of the study, conducting the literature review and research framework, supervision of the research process, and reviewing and editing the paper.

Maryam Naveed (2nd author): Questionnaire design, conducting data collection, and writing and editing parts of the manuscript.

Hassan Shah Khan (3rd author): Performing data analysis using Python software including Pandas, NumPy, SciPy, and Matplotlib, visualization of results, interpretation of results, and preparing the methodology and results sections.

Sobia Ayaz (4th author): Support in data validation, preparing figures and tables.

References

[1]. I. Ajie, "A review of trends and issues of cybersecurity in academic libraries," *Library Philosophy and Practice*, 2019.

[2]. S. Balasubramanian and N. Tamilselvan, "Exploring the potential of artificial intelligence in library services: A systematic review," *International Journal of Library & Information Science*, vol. 12, no. 1, 2023, doi: 10.17605/OSF.IO/S9RWD.

[3]. A. Goetsch, "Creating a culture of security in the University of Maryland libraries," *portal: Libraries and the Academy*, vol. 1, no. 4, pp. 455–464, 2001. https://doi.org/10.1353/PLA.2001.0074.

[4]. K. Kont, "Libraries and cyber security: The importance of the human factor in preventing cyber attacks," *Library Hi Tech News*, vol. 41, no. 1, pp. 11–15, 2024, doi: 10.1108/LHTN-03-2023-0036.

[5]. A. Aregbesola and E. L. Nwaolise, "Securing Digital Collections: Cyber Security Best Practices for Academic Libraries in Developing Countries," *Library Philosophy and Practice (e-journal)*, no. 7822, 2023.: https://digitalcommons.unl.edu/libphilprac/7822

[6]. M. O. Igbinovia and B. C. Ishola, "Cyber security in university libraries and implication for library and information science education in Nigeria," *Digital Library Perspectives*, vol. 39, no. 3, pp. 248–266, 2023, doi: 10.1108/DLP-11-2022-0089.

[7]. N. A. M. Roni, B. Hassan, and M. K. M. Napiah, "Impact of ICT on privacy and personal data protection in two Malaysian academic libraries," in *Asia-Pacific Conf. Library & Inf. Educ. Practice*, 2011.

[8]. S. Krueger, "Academic Librarians in Canada Concerned About Online and Patron Privacy but Lack Knowledge About Institutional Procedures and Policies", EBLIP, vol. 14, no. 2, pp. 116–118, Jun. 2019.: https://doi.org/10.1016/j.lisr.2018.05.002

[9]. W. Aljohni, N. Elfadil, M. Jarajreh, and M. Gasmelsied, "Cybersecurity awareness level: The case of Saudi Arabia university students," *International Journal of Advanced Computer Science and Applications (IJACSA)*, vol. 12, no.32021http://dx.doi.org/10.14569/IJACSA.2021.0120334.

[10]. M. F. Baharuddin, A. Jalil, Z. M. Amin, F. Rahmad, and S. M. Shuhidan, "Digital literacy and cybersecurity in higher education: The unseen power of academic librarians," *International Journal of Evaluation and Research in Education (IJERE)*, vol. 14, no. 6, pp. 4404–4417, 2025, doi: 10.11591/ijere.v14i6.34916

[11]. F. Quayyum, D. S. Cruzes, and L. Jaccheri, "Cybersecurity awareness for children: A systematic literature review," *International Journal of Child-Computer Interaction*, vol. 30, p. 100343, 2021.: https://doi.org/10.1016/j.ijcci.2021.100343.

[12]. K. Arlitsch and A. Edelman, "Staying safe: Cyber security for people and organizations," *J. Library Administration*, vol. 54, no. 1, pp. 46–56, 2014. Available: https://doi.org/10.1080/01930826.2014.893116.

[13]. B. Oladokun, E. Oloniruha, D. Mazah, and O. Okechukwu, "Cybersecurity risks: A sine qua non for university libraries in Africa," *Southern African Journal of Security*, vol. 2, Mar. 2024, pp. 1–14, doi: 10.25159/3005-4222/15320.

[14]. S. O. Akor, C. Nongo, C. Udofot, and B. D. Oladokun, "Cybersecurity awareness: Leveraging emerging technologies in the security and management of libraries in higher education institutions," *Southern African Journal of Security*, vol. 2, pp. 1–14, 2024, doi: 10.25159/3005-4222/16671

[15]. M. Y. Ali, "Cybersecurity threats in Pakistani academic libraries in the era of artificial intelligence," *The International Information & Library Review*, vol. 57, no. 2, pp. 204–210, 2025, doi: 10.1080/10572317.2025.2479289.

[16]. S. K. W. Fakeh et al., "Information security awareness amongst academic librarians," *J. Applied Sciences Research*, vol. 8, no. 3, pp. 1723–1735, 2012.

[17]. K.-R. Kont, "The role of libraries in creating a safer cyberspace: Awareness of Estonian library employees in information security," *The International Information & Library Review*, vol. 56, no. 2, pp. 135–149, 2024.: https://doi.org/10.1080/10572317.2024.2315630.

[18]. L. Kavak, "Impact of information security awareness on information security compliance of academic library staff in Türkiye," *The Journal of Academic Librarianship*, vol. 50, no. 5, p. 102937, 2024, doi: 10.1016/j.acalib.2024.102937

[19]. S. Al-Janabi and I. Alshourbaji, "A study of cyber security awareness in educational environment in the Middle East," *J. Inf. Knowl. Manag.*, vol. 15, p. 1650007, 2016. Available: https://doi.org/10.1142/S0219649216500076.

[20]. G. Farid, N. F. Warraich, and S. Iftikhar, "Digital information security management policy in academic libraries: A systematic review (2010–2022)," *Journal of Information Science*, vol. 51, no. 4, pp. 1000–1014, 2023, doi: 10.1177/01655515231160026.

[21]. S. Panda and N. Kaur, "Cyber sentinels: Exploring the cybersecurity awareness of Indian library professionals," in *Applications of Artificial Intelligence in Libraries*, IGI Global Scientific Publishing, 2024, pp. 78–108, doi: 10.4018/979-8-3693-1573-6.ch004.

[22]. I. M. Inam, N. Shaheen, W. A. Channar, M. Ali, Z. Lakho, and A. Ahmed, "Cyber-security challenges in digital libraries," *Review Journal of Social Psychology & Social Works*, vol. 3, no. 1, pp. 344–350, 2025, doi: 10.71145/rjsp.v3i1.102

[23]. R. Armas and H. Taherdoost, "Building a cybersecurity culture in higher education: Proposing a cybersecurity awareness paradigm," *Information*, vol. 16, no. 5, p. 336, 2025, doi: 10.3390/info16050336.

[24]. K. Komane, L. Khoza, and F. Radebe, "A Conceptual Framework for Cybersecurity Awareness," *J. Cyber Secur.*, vol. 7, no. 1, pp. 79–108, 2025. https://doi.org/10.32604/jcs.2025.059712

[25]. B. Wambui, M. Mwinji, and H. Nyambura, "AI-Driven Cybersecurity Framework for Safeguarding University Networks from Emerging Threats," *J. Cyber Secur.*, vol. 7, no. 1, pp. 463–482, 2025. https://doi.org/10.32604/jcs.2025.069444

[26]. E. Pasipamire, "Building a culture of cybersecurity awareness in libraries: A systematic review of best practices and frameworks," in *Proc. European Conference on Cyber Warfare and Security*, Academic Conferences International Limited, Jun. 2025, pp. 510–519, doi: 10.34190/eccws.24.1.3608.

[27]. C. K. Gajbhiye, "Impact of artificial intelligence (AI) in library services," *Int. J. Multidisciplinary Res.*, vol. 6, no. 3, pp. 1–13, 2024.

[28]. C. D. Nguyen, "Digital cultural heritage in the crossfire of conflict: Cyber threats and cybersecurity perspectives," *Insights*, vol. 37, no. 1, 2024. :https://doi.org/10.1629/uksg.647

[29]. K. Ghimire, "Cyber-attack issues: Laws & policies and the role of librarians," *Access: An International Journal of Nepal Library Association*, vol. 2, no. 1, pp. 216–234, 2023, doi: 10.3126/access.v2i01.59002.

[30]. M. A. Alqahtani, "Factors affecting cybersecurity awareness among university students," *Applied Sciences*, vol. 12, no. 5, p. 2589, 2022.: https://doi.org/10.3390/app12052589

[31]. M. Khader, M. Karam, and H. Fares, "Cybersecurity awareness framework for academia," *Information*, vol. 12, no. 10, p. 417, 2021: https://doi.org/10.3390/info12100417

[32]. A. O. Dunmade and A. Tella, "Libraries and librarians' roles in ensuring cyberethical behaviour," *Library Hi Tech News*, vol. 40, no. 7, pp. 7–11, 2023, doi: 10.1108/LHTN-04-2023-0068.

[33]. O. Adenike and R. Alabi, "Awareness and perception of cybersecurity among librarians in federal universities in South-West, Nigeria," *Journal of Library Services and Technologies*, vol. 5, no. 3, pp. 90–104, 2023, doi: 10.47524/jlst.v5i3.91.

[34]. E. M. Corrado, "Cybersecurity and libraries," *Technical Services Quarterly*, vol. 41, no. 1, pp. 82–95, 2024, doi: 10.1080/07317131.2023.2300530.

[35]. R. H. Ajagekar, "Cyber security and its application in academic libraries," *Aayushi International Interdisciplinary Research Journal (AIIRJ)*, vol. 11, no. 12, pp. 41–47, Dec. 2024

[36]. A. M. Alhaif, "Training needs of information specialists at Saudi universities libraries to achieve cybersecurity requirements," *International Journal of Education and Information Technologies*, vol. 17, pp. 38–50, 2023, doi: 10.46300/9109.2023.17.5

[37]. A. A. Hakami, "The role of public librarians in reducing cybercrime: Literature review," *Public Library Quarterly*, pp. 1–14, 2025, doi: 10.1080/01616846.2025.2600686.

[38]. O. Onunka, T. Onunka, A. A. Fawole, I. J. Adeleke, and C. Daraojimba, "Library and information services in the digital age: Opportunities and challenges," *Advances in Information Management*, vol. 7, no. 2, pp. 113–121, 2023, doi: 10.26480/aim.02.2023.113.121

[39]. P P. Raghavaiah and S. Karnati, "The importance of cybersecurity in academic libraries in modern age," in *Proc. 12th International Library and Information Professionals Summit (I-LIPS)*, Greater Noida, India, 2025.

[40]. Z. Ibrahim and G. Kotoroi, "Overcoming challenges in implementing electronic security systems at Mzumbe University Library: Strategic pathways for improvement," *American Journal of Information Science and Technology*, vol. 9, no. 1, pp. 1–14, 2025, doi: 10.11648/j.ajist.20250901.11.