

Human Factors and Cybersecurity Awareness in Pakistani Universities: A Behavioral and Risk Analysis Study

Dr. Abdul Khaliq

abdulkhaliq@cuvas.edu.pk

Assistant Professor, Department of Social and Allied Sciences, Cholistan University of Veterinary and Animal Sciences, Bahawalpur

Danyal

malikdanyal7864119@gmail.com

BS Computer Science Scholar, Department of Computer Science, Cholistan University of Veterinary and Animal Sciences, Bahawalpur

Rameez Ahmad

rameezahmedra1@gmail.com

BS Computer Science Scholar, Department of Computer Science, Cholistan University of Veterinary and Animal Sciences, Bahawalpur

Corresponding Author: Dr. Abdul Khaliq abdulkhaliq@cuvas.edu.pk

Received: 09-02-2026

Revised: 24-02-2026

Accepted: 12-03-2026

Published: 26-03-2026

ABSTRACT

Cybersecurity has become a major challenge in Pakistani universities due to the speedy digital transformation. In the context of universities, they exist in a very open digital space, with students, faculty, administrative staff and even IT personnel all accessing university systems on regular basis via interconnected networks and their personal devices. This study focuses on the impact of human factors on the cybersecurity awareness and vulnerabilities in Pakistani Universities. The research examines the primary cyber threats such as phishing attacks, use of weak passwords, ransomware, social engineering, credential sharing and unauthorized access to institutional systems. Descriptive and analytical research design was used in the study, and behavioral risk analysis, survey and semi-structured interviews were employed to assess cybersecurity awareness and risky practices of University Stakeholders. The results indicate that factors such as low cybersecurity awareness, insufficient institutional training, weak policy enforcement and unsafe online behaviors play a major role in the cybersecurity vulnerabilities in academic environments. The study states that technical security systems are not enough if there are no continuous awareness programs and behavioral training. Therefore, a human-centred cybersecurity awareness framework is suggested to enhance the cyber security resilience and encourage secure digital practices in Pakistani universities.

Keywords: Cybersecurity Awareness, Human Factors, Phishing Attacks, Pakistani Universities, Behavioral Risk Analysis

INTRODUCTION

One of the most important issues facing the universities in the world today is cyber security. Universities have significant digital resources and sensitive academic records, financial data, research data and personal information about students and staff. The universities in Pakistan are increasingly adopting digital systems in online admission, learning management system, digital libraries, virtual classrooms, and administration. This digital transformation has enhanced learning accessibility and efficiency, but has also made education very vulnerable to cyber threats (Hadlington, 2017).

The university is a place of open-access digital environments, which differ from corporate organizations that have strict cyber security controls and centralized monitoring systems. Students often plug their personal devices into school networks, professors post research online for students to access, and staff members discuss sensitive information via email. This openness brings about a dynamic cyber security landscape in which human behavior has a direct impact on institutional cybersecurity vulnerabilities.

These threats are not to be taken lightly, as evidenced by several cybersecurity incidents reported in Pakistani universities. An example of such a phishing attack involved universities that appeared to be from the university itself asking for students' and employees' logon information. In some instances fake fee payment notifications and fraudulent financial requests were sent by compromised accounts. In addition, ransomware attacks temporarily affected access to examination records, student databases, online learning systems etc. on the University's servers. Unauthorized access to student portals and abuse of shared login credentials are also a testament to a lack of cybersecurity awareness and/or human behavior. Human factors are the psychological, behavioural and social factors that affect the way that people interact with technology and security systems. Numerous cybersecurity research studies have come out showing that technical controls are not enough if users don't do their part in practice. There are numerous user habits that can create cyber risk exposure, including the use of weak passwords, visiting suspicious web links, neglecting to update software, and handing over passwords (Parsons et al., 2017).

The Cyber Security Awareness programs in universities are limited and inconsistent in Pakistan. Many institutions offer only general orientation sessions on issues of digital security, and students and staff rely mainly on personal experience and not on cybersecurity education. In many cases, faculty is more focused on academic activities than on cybersecurity practices, and administrative staff lack time due to pressure, which creates a chance for cybersecurity negligence. Behavioral risk analysis is a very useful way of seeing how user attitudes, habits and perceptions can be related to cybersecurity threats. The technique of social engineering relies on trust and authority relationships found in academic environments. Emails sent from department heads or from IT administrators are likely to be responded to immediately without necessarily checking it out. Likewise, students can pass their logins to their fellow students for academic reasons without realizing that they are exposing the system to security risks.

The aim of this study is to review the cybersecurity awareness and human behavioural risks in the context of Pakistani Universities, focusing on actual cyber incidents, the nature of the insecure practices, and the institutional responses. The study highlights the need for ongoing awareness, behavior change, and accountability within the institutions themselves as part of cybersecurity resilience in higher education.

Background of Study

The digital technologies have been rapidly expanding in Higher Education (HE) making its academic environment in Pakistan completely different. Digital systems are becoming more vital to universities for teaching, administration, communication, and collaboration in research. While these technological developments enhance operation efficiency, they also leave institutions vulnerable to new and changing cybersecurity threats. Universities are becoming an appealing target for a cybercriminal because they hold a considerable amount of sensitive information, especially with the growing reliance on digital platforms. Most cybersecurity incidents in educational institutions are caused by human vulnerabilities, and not by system failures. Studies show that users often misjudge the threats of cyber security and do not practice safe online habits (Parsons et al., 2017). There is a lack of awareness of cybersecurity, no training programs in Pakistani universities and poor enforcement of policy.

Management of the cybersecurity of university networks is also complicated because of their open nature. Students routinely use their personal laptops and mobile devices to access University systems and faculty

and administrative staff share confidential information in electronic systems. All these activities can lead to phishing attacks, malware infections, credential theft, and unauthorized access. Therefore, a human-centric cyber security framework is required that will tackle awareness, behaviour and risk management within the academic arena.

Statement of the Problem

Given the lack of awareness, the insecure behaviour of users and the lack of cybersecurity practices at the institutions, Pakistani universities are also experiencing the rising cybersecurity threats. Many universities are vulnerable to phishing attacks, social engineering, poor password habits and unauthorized access to their systems, even though they have taken steps to ensure their technical security.

The biggest issue is that the human factor remains the biggest cause of cyber security incidents in higher education institutions. Students, faculty and administrative personnel may not be equipped with sufficient cybersecurity knowledge, or aware of the digital threats. In addition, many universities are not doing on-going awareness or simulated cybersecurity drills for user behavior and preparedness. This means that cyberattacks have the potential to result in financial losses, data breaches, disruption of academic operations, loss of reputation, and unauthorized release of sensitive data. Consequently, there is an urgent need to explore the human behavioral risks and need for developing structured cybersecurity awareness strategies particular to Pakistani Universities.

Objectives of the Study

Following are the objectives of the study:

1. To investigate Human factors affecting Cyber security Awareness and Behavior in Pakistani Universities.
2. To determine the frequent cyber security dangers and risky practices in HEIs of Pakistan.
3. To suggest a human-centric cybersecurity awareness framework for enhancing institutional cyber resilience.

Research Questions

Following questions cover objectives of the study:

1. How Human Factors can affect Cyber Vulnerabilities in Universities of Pakistan?
2. What are the top behavioral Cybersecurity threats in higher education institutions?
3. What are the steps that Universities can take to enhance cybersecurity awareness and secure digital behavior of students and staff?

Importance of the Study

This study has significance as it represents the importance of Cyber Security awareness among the Higher Education Institutions in Pakistan. The study adds to the body of knowledge on the human factors that affect institutional cybersecurity risks and illustrates the need to address the cybersecurity issues in academic environments beyond just technical solutions.

The results will be useful for the university administrators, IT departments, policy makers, students and faculty members to identify the important vulnerabilities and suggest effective awareness strategies. The research also offers valuable insights into designing institutional cyber security training, policies and risk management practices for Pakistani Universities.

In addition, the research adds to the academic literature in the field of Cyber Security in developing countries by highlighting the importance of incorporating behavioral analysis into Cyber Security risk management.

Delimitations of the Study

This study only examines human factors and cybersecurity awareness in Higher Education Institutions "HEIs" in Pakistan. The study will particularly focus on behavioral cybersecurity risks amongst students, faculty and administrative staff, such as phishing attacks, weak password practices, social engineering, ransomware threats and sharing of credentials within University settings.

The study focuses mainly on awareness and behavioral risk analysis of cyber security, as opposed to the detailed technical assessment of the cyber security infrastructure or cybercrime incident forensic analysis. In the context of limited time and resources, the study was limited to selected universities from Pakistan and might not cover all universities or any other organizational sectors of Pakistan. However, the research offers useful insights into the importance of human behavior in cybersecurity resilience in academic institutions.

LITERATURE REVIEW

Conceptual Framework

This study's conceptual framework is derived from the human factors and cybersecurity risk in Pakistani Universities. Human factors encompass a range of factors, such as students' and employees' awareness, attitudes, password practices, phishing awareness, risk perception, and digital literacy and adherence to institutional cyber-security policies. These factors directly affect cybersecurity behavior and if users will use safe or unsafe digital practices.

Weak cybersecurity awareness, overconfidence in digital skills, poor password management and lack of continuous training are all seen as factors that add to institutional cyber risks, including phishing, ransomware, unauthorized access, credential misuse, and data breaches. However, through consistent awareness efforts, simulated phishing exercises, robust authentication protocols, and policy enforcement, secure behaviors can be fostered, and cyber risks can be minimized. The uploaded study also highlights that phishing attacks, weak passwords, ransomware threats, and misuse of common passwords are large cybersecurity issues in Pakistani Universities.

Theoretical Framework

The Protection Motivation Theory (PMT) and the Theory of Planned Behavior (TPB) are used to support this study. Protection Motivation Theory is a theory of response to cyber threat through perceived severity, perceived vulnerability, response efficacy, and self-efficacy. When students and employees know the severity of cyberattacks and feel confident in their ability to protect themselves, they are more likely to take care in a University environment.

Behavior in cybersecurity is understood based on the Theory of Planned Behavior, which is, attitudes, subjective norms, and perceived behavioral control. When students and staff see the relevance of cybersecurity, see others practicing safe behaviors, and are confident using security tools, they are more likely to practice secure behaviors. Attitudes to cybersecurity and risky online behaviour are strongly linked (Hadlington 2017), and Parsons et al. (2017) pointed out that human awareness and behaviour are key to information security performance.

Pakistani Context: Related Studies

Khan et al. (2022) explored Cyber security and risky Internet behaviors of undergraduate students in Pakistan. They concluded that there is a scarcity of cybersecurity behavior research in developing countries, and they also noticed that there are differences in risky cyber behavior among the students in Pakistan based on various demographic, socioeconomic, and digital divide factors.

According to the Ministry of Federal Education and Professional Training Pakistan (2023), cybersecurity awareness training is crucial, and some of the primary issues faced by users in educational institutions include phishing, weak passwords, and unsafe online practices. According to the study on Pakistani Universities uploaded, the students, faculty members and administrative staff are still vulnerable to phishing attacks, ransomware, shared credentials and weak cybersecurity practices because of insufficient training and weak enforcement of policies.

The findings from the study of social engineering attacks in Pakistan also suggest that, in order to minimize cyber attacks in organizations and educational institutions, it is important to raise awareness about phishing, use secure passwords, and adhere to safe browsing practices. Anjum (2019) analyzed cybercrime in Pakistan and included awareness of cybercrime by university students, proving that the awareness of cybercrime is a crucial aspect of cybercrime prevention at the student level.

The ReCyP:HER initiative “Rethinking Cybersecurity in Pakistan—Human Factors” is a testament to the increasing focus on human behaviour in the field of cyber security at the academic and institutional level in Pakistan.

Awareness, psychology and user behaviour are emerging themes in national cybersecurity and the National Centre for Cyber Security Pakistan has encouraged study in this field. Ahmead (2024) studied risky online behaviors and awareness of cybercrime, and reported that many respondents had experienced cybercrime or had known someone who did, and that there was still a significant lack of awareness.

Weak awareness, overconfidence and lack of continuous training were found to be the major institutional vulnerabilities in a recent article in Pakistan about human factors and cybersecurity awareness in universities, with a focus on students, faculty and administrative staff in Bahawalpur. In conclusion, Pakistani studies reveal that awareness of cyber security in universities is still not developed well and universities require continuous, structured and behavior focused cyber security programs.

International context: related studies

Hadlington (2017) conducted a study on human factors in cyber security and discovered a correlation between impulsivity, internet addiction, and attitudes towards cyber security and risky cybersecurity behaviors. Parsons et al. (2017) have created the Human Aspects of Information Security Questionnaire and have highlighted the importance of employee awareness, attitude and behaviour in the field of information security.

Al-Janabi and Al-Shourbaji (2016) conducted a study on Cyber security awareness in educational contexts and their results revealed the absence of an effective Cyber security awareness program and policy enforcement in many educational institutes. Alqahtani (2022) evaluated the cybersecurity awareness of university students and results indicated that: Password security, Browser security, and social media behavior significantly affect cybersecurity awareness.

Cybersecurity was identified as a significant concern for higher education, and phishing and ransomware attacks were cited as two of the most prevalent attacks on higher education institutions globally by EDUCAUSE. According to the systematic review on cybersecurity in higher education, phishing is among the most prevalent threats in Higher Education institutions as well as human behavior determines a significant part of the cyber risk in Higher Education institutions.

A study on cybersecurity threats faced by universities revealed that ransomware is a frequent external threat and misuse of access and insider threats are significant threats in educational institutions. Armas (2025) suggested a cybersecurity awareness and training model for universities, and the establishment of cybersecurity culture within the university community and students.

Bottyán (2025) examined the cyber security behaviors of university students regarding ransomware attacks and identified phishing vulnerability, credential practices, software hygiene and threat perception as significant risk factors. In his study, Raju (2022) explored the preparation of the university students in cybersecurity awareness through digital platforms and stated that the awareness of personal information protection, cyberbullying and online safety is vital in current education.

Research Gap

In the literature reviewed, it has been demonstrated that human behavior is a key source of vulnerability in cybersecurity in universities. Cyber security awareness, phishing activities, password habits, threats of ransomware, and training programs in higher education have been studied internationally. But few studies have been done on an institutional level for Pakistani universities particularly in relation with students, faculty and institutional practices.

Most of the research regarding cybercrime awareness has been conducted in general or on students' behavior and not many studies have been conducted using a combined approach of behavioral and risk analysis to examine cybersecurity awareness. Limited information is also available on structured, continuous and human-centred cybersecurity awareness frameworks for HEIs in Pakistan. The current study, therefore, aims to bridge this gap through an analysis of human factors, behavioural risk and cybersecurity awareness in Pakistani Universities and then, proposes a practical awareness framework for local academic settings.

RESEARCH METHODOLOGY

Research Design

The present research uses descriptive and analytical approach to investigate the awareness, human behavior and digital risk factors in Pakistani Universities. The descriptive dimension of the study aims to identify common cyber risks, awareness of cyber risks, and risky online behaviours of students, faculty, administrative and IT staff. The analytical dimension assesses human factors that impact institutional cybersecurity vulnerabilities and how human behavior patterns impact cybersecurity resilience in academic settings.

An approach of a behavioral risk analysis is used in the study since cybersecurity incidents in universities are not necessarily due to technical failures in the system, but to human mistakes. Behavioral risk analysis can be used to better understand user interactions with digital systems, how users perceive cyber threats and how they react to cyber security policies and practices. Descriptive and analytical research designs are suitable for research that focuses on examining behavioral patterns, institutional practices and risk-related issues within the organizational context, according to Creswell and Creswell (2018).

The research also adopts a qualitative-oriented approach and the use of assessment methods based on surveys to analyze the awareness of cyber security and the vulnerabilities of humans in universities. The study specifically examines the behaviours linked to the susceptibility to phishing, password practice, social engineering risk, sharing of credentials and digital security awareness among the university stakeholders (Hadlington, 2017).

Research Approach

This study adopts a mixed qualitative and behavioral assessment methodology to assess the cybersecurity awareness and human vulnerabilities in Pakistani universities. Data collection was conducted using a qualitative approach to gain in-depth information on user perception, awareness, institutional cybersecurity culture, and risky use on digital devices. Behavioral assessment methods were integrated in order to assess user's responses to cyber threats or security-related situations in academic settings.

This choice was made because there are psychological, social, and organizational factors that impact cybersecurity behavior and cannot be fully understood through technical analysis. Saunders et al (2019) noted that the qualitative and behavioural methods are very effective in studying human attitudes, perceptions and practices in organizational studies. Hence, the chosen method of research will give a holistic perspective on human factors in the context of cybersecurity risks in higher education institutions.

Population of the Study

The study will focus on students and faculty staff, administrative staff, and IT professionals from various Pakistani universities. These groups were chosen for the reason that they have frequent interaction with institutional digital systems and have a direct influence in maintaining or impeding cybersecurity within academic environments.

Students are a major component of a university's network users, often using personal devices to access online learning systems, e-libraries, email systems, etc. and social media apps. Institutional communications, financial information, and sensitive student records are handled by administrative staff, whereas academic materials and research data are regularly shared by faculty members by means of online platforms. IT staff were also selected due to their role in running systems for the cybersecurity of the institution, technical support and network administration (Parsons et al., 2017).

The presence of various stakeholder groups enabled the study to gather a variety of viewpoints about cybersecurity awareness, risky cyber behaviors, institutional practices, and cybersecurity issues in Pakistani universities.

Sample technique and sample size

The participants involved in the study were selected using a purposive sampling technique with the goal of obtaining information from individuals who have knowledge and experience in digital systems, cyber security practices, and institutional technology usage. The method of purposive sampling is suitable for

behavior and exploratory studies in which the participants of the study are chosen related to the objective of the study (Bryman, 2016).

The respondents of the study were selected from various Universities of Pakistan such as students, faculty, administrative staff and IT professionals. The participants were selected due to their direct engagement with institutional digital infrastructures, and due to their exposure to cybersecurity related activities. The selected sample yielded interesting information on phishing attacks, the use of passwords, the risks of social engineering, awareness levels and institutional cybersecurity culture.

Data Collection Methods

The study employed survey and semi-structured interviews as the main tools for data collection. Survey was the selected method of researching data on cybersecurity awareness, online behaviors, phishing awareness, password practices, and attitudes about cyber risks. Structured questionnaires were created to assess the participants' awareness of the risks of cybersecurity and their adherence to institutional security practices.

Selected faculty, IT staff, and administrative personnel were interviewed on a semi-structured basis to gain detailed qualitative insights into the challenges faced by the institution in terms of cybersecurity, how policies are enforced, and the vulnerabilities of human behavior. Semi-structured interviews are good for behavioral and exploratory studies as they give the participants the freedom to elaborate on experiences and perceptions whilst keeping the consistency of the data collection (Bryman, 2016).

Behavioral assessment techniques were also used to assess phishing susceptibility, password-sharing behaviour, response to suspicious emails and general digital risk perception among the participants. Clicking on links you don't know, using weak passwords, sharing passwords, ignoring software updates and even answering suspicious online requests were all analyzed. These assessments were used to identify key human vulnerabilities in the field of cybersecurity in universities (Hadlington, 2017).

Data Analysis Techniques

Thematic analysis and comparative analysis methods were used in analysing the collected data. Using the thematic analysis approach, patterns, themes, and behavioral trends for cybersecurity awareness, phishing behavior, password practices, and institutional cybersecurity culture were identified. This method enabled a researcher to classify responses of the participants into meaningful themes related to human factors vulnerability in cybersecurity.

The differences in cybersecurity awareness and digital practices were compared between the different groups (students, faculty members, administrative staff, and IT personnel). During the analysis, key risk indicators, including password sharing, phishing response behaviors, weak authentication practices, awareness, software update behaviors, and policy compliance, were explored (Parsons et al., 2017).

The results were analyzed with the aim of evaluating the role played by human behavior in the vulnerabilities of the institutions in the cyber space, as well as areas that would need to be raised about. The analysis also contributed in proposing a Human centered Cyber security awareness framework for the HE environment in Pakistan.

RESULTS AND DISCUSSION

Based on the results of the present study, it is found that the knowledge and awareness of cyber security in Pakistani Universities is low and inadequate for students, faculty, administrative and IT staff. The research suggests that people continue to be a major factor in cybersecurity challenges in Higher Education institutions. A high number of participants showed poor awareness of cyber attacks like phishing, ransomware, social engineering, stealing passwords, or unauthorized access to information technology. This aligns with the outlook of Parsons et al. (2017) who stressed how lack of cybersecurity awareness and bad digital practices play a crucial role in the exposure of organizations to cyber risks.

The study revealed that the use of weak password management practices is very prevalent among University users. Many respondents indicated that they use simple or repetitive passwords across various online platforms for ease of use. Several also said they shared username and password with classmates, colleagues or friends for accessing academic sources and institutional systems. These practices can heighten the likelihood of breaches, misuse of credentials and unauthorized access to institutional data. Similarly, Hadlington (2017) identified risky online activities and bad habits with passwords as being strong indicators of cybersecurity vulnerabilities and insecure online habits.

Another significant result of the study is that there was not a lot of knowledge about phishing attacks and social engineering techniques among the participants. Numerous respondents said they had trouble spotting deceptive emails, fake login pages, or fake institutional communications. Some respondents said they primarily use personal judgement rather than institutional cybersecurity policies to respond to digital communications. This behavior renders academic users highly susceptible to phishing attacks that leverage relationships of trust, urgency and authority in such environments. A major problem that is common in educational institutions is that users are not aware of the sign of phishing and the methods used to verify online information (Al-Janabi & Al-Shourbaji, 2016).

The findings also indicate that the major behavioural risks in Pakistani universities are delayed software updating, weak authentication practices and negligence of cybersecurity protocols. Some of the participants admitted that they did not bother to install software updates or used an outdated anti-virus solution because it was inconvenient or they were unaware of the need for software updates. Users' perception of risks associated with cybersecurity was low in many cases with the potential consequences of insecure digital behavior underestimated. Furthermore, according to Khan et al. (2022), institutional training is not widespread in developing countries, and individuals may feel very confident with their own skills and knowledge regarding cybersecurity.

The study also concluded that the universities that conducted regular cybersecurity awareness sessions, training workshops, and simulated phishing attacks had significantly higher cybersecurity resilience and safer behavior of users. Participants who were from institutions where ongoing awareness campaigns are carried out were more aware of password security, how to recognize phishing and secure online communication practices. These results indicate that multiple exposures to cybersecurity education have a positive impact on user awareness and behavioral improvement. EDUCAUSE (2023), highlighted that institutions that have ongoing cybersecurity awareness programs have a better level of institutional readiness to cyber threats.

What's more, the results reveal that institutional cybersecurity policies are frequently in place, but do not appear to be effectively enforced. Many of the respondents indicated that universities are not offering much help except the orientation sessions on cybersecurity. Weaknesses identified within institutional vulnerabilities included inadequate monitoring systems, lack of mandatory cybersecurity training and lack of adequate incident reporting procedures. The study thus emphasizes the importance of setting up and

enforcing formal and enforceable cybersecurity frameworks with the support of leadership and institutional accountability within universities.

As demonstrated in the behavioral analysis performed in this study, cybersecurity resilience cannot solely rely on technical protections including firewalls, antivirus software and encryption systems. The human element continues to play an important role in institutional cybersecurity performance. The potential for exploiting academic environments by cybercriminals remains due to unsafe digital habits, low awareness and poor compliance with cybersecurity practices. The results are consistent with other international studies that showed that one of the main causes of cyber security incidents in organizations and educational institutions is human errors (Parsons et al., 2017).

In conclusion, the findings suggest that there is a need for a holistic, human-centric approach to cybersecurity in Pakistani universities, emphasizing the importance of awareness, behavioral training, policy implementation, and ongoing risk assessment. A strong cybersecurity culture is a crucial component of the resilience of higher education institutions, their data, and their digital learning spaces in the face of cyber threats.

CONCLUSION

Based on the findings of the current study, it is concluded that human factors are an important factor in defining the vulnerabilities in the Pakistani universities' cybersecurity field. While more and more universities are utilizing digital tools for their academic, administrative and research processes, many of these institutions are still vulnerable to cyber threats due to a lack of cybersecurity awareness, insecure digital behavior and inadequate institutional security practices. The results of the study show that some of the most prevalent behavioral threats in a university environment include phishing attacks, weak password practices, social engineering, credentials sharing, and inadequate adherence to cybersecurity policies.

The study also finds that merely having a technical security system is not enough if those using them are not securely using their digital devices. With the lack of cyber awareness and cyber responsibilities of students, faculty members and administrative staff, firewalls, anti-virus software, encryption systems, and access-control mechanisms are much less effective. These findings agree with the study of Parsons et al (2017), they stated that human behavior is one of the most vulnerable points of information security systems. Also, Hadlington (2017) pointed towards risky online behaviors and overconfidence in digital literacy as a major element of cybersecurity vulnerabilities.

One key finding is the need for a human-centered approach to cybersecurity resilience in higher education, which can be achieved through ongoing awareness initiatives, behavioral training, policy enforcement and institutional accountability. Institutions with regular cybersecurity workshops, phishing simulations, and awareness campaigns revealed a higher level of cybersecurity preparedness and safer user behavior, whereas institutions that did not offer such events had lower levels of preparedness and safer user behaviors. The results thus highlight the need to incorporate behavior risk analysis in institutional cybersecurity plans to enhance cyber-resilience in academic settings.

In addition, the study states that there is a need for structured governance processes, leadership commitment, continuous training and proper implementation of policies in Pakistani universities to tackle cybersecurity issues. Apart from safeguarding institutional information and academic communication systems, human-centric cybersecurity approaches will be necessary to assure continuity of educational operations and public confidence in the systems of digital higher education.

RECOMMENDATIONS

In light of the findings of the present research, it is suggested that Pakistan universities can take steps towards continuous cyber security awareness and training courses for students, faculty members, administrative staff, and IT staff. Continuous cybersecurity training programs can have a profound impact on enhancing awareness about phishing attacks, password hygiene, safe browsing habits, and social engineering threats. Periodic simulated phishing exercises, cyber hygiene workshops, and awareness campaigns should be held to reinforce the safe use of digital technologies at the University. Continuous cybersecurity awareness programmes are crucial in enhancing institutional readiness to address the shifting cyber threats in higher education institutions, as noted by EDUCAUSE (2023).

The study also recommends that universities should improve their institutional policies on cyber security and make sure that these policies are implemented and enforced. All University systems and digital platforms must implement secure authentication practices like multi-factor authentication, strong password requirements, and regular password updates. Further, it is crucial for institutions to have well-defined cybersecurity reporting protocols and cybersecurity incident response plans in place to ensure that the effects of a cyberattacks and incidents of unauthorized access are minimized. Al-Janabi and Al-Shourbaji (2016) stated that if there is an effective cybersecurity policy and an institutional monitoring system, the behavioral vulnerabilities are significantly reduced in educational institutions.

Furthermore, university campuses should have a team of people who are specifically tasked with monitoring digital threats, responding to security incidents, risk assessment, and supporting university's cybersecurity operations. These teams should be able to cooperate with the university management and information technology departments to enhance the cyber security system and foster a cyber security culture in universities as a whole. The study also emphasizes the need for incorporating behavioral risk assessment and integrating into institutional cybersecurity planning and decision making processes.

In addition, universities in Pakistan need to have a common cyber security awareness framework, institutional guidelines and training models, which can be established in collaboration with Higher Education Commission. National level cyber security frameworks can provide support to universities to ensure that there are consistent security standards, awareness programs and risk management strategies throughout the higher education sector. This can also help to develop policies, provide technical training, and build cybersecurity competencies in Pakistani universities.

Lastly, future researchers must delve into other aspects of cybersecurity awareness in higher education such as cybersecurity AI, behavioral analytics, ethics of digital information, and the integration of new technologies in cybersecurity management. Future mass-scale quantitative research can also yield greater understanding of the link among human behavior, institutional culture, and cybersecurity resilience in academic settings.

REFERENCES

- Al-Janabi, S., & Al-Shourbaji, I. (2016). A study of cyber security awareness in educational environment in the Middle East. *Journal of Information & Knowledge Management*, 15(1), 1650007. <https://doi.org/10.1142/S0219649216500076>
- Alqahtani, M. A. (2022). Factors affecting cybersecurity awareness among university students. *Applied Sciences*, 12(5), 2589. <https://doi.org/10.3390/app12052589>

- Anjum, U. (2019). *Cyber crime in Pakistan: Detection and punishment mechanism* (MPhil thesis). Pakistan Institute of Development Economics.
- Bryman, A. (2016). *Social research methods* (5th ed.). Oxford University Press.
- Creswell, J. W., & Creswell, J. D. (2018). *Research design: Qualitative, quantitative, and mixed methods approaches* (5th ed.). Sage Publications.
- EDUCAUSE. (2023). *Top IT issues in higher education*. [EDUCAUSE Official Website](https://www.educause.edu/technology-top-issues)
- Hadlington, L. (2017). Human factors in cybersecurity: Examining the link between internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviors. *Heliyon*, 3(7), e00346. <https://doi.org/10.1016/j.heliyon.2017.e00346>
- Khan, N. F., Ikram, N., Saleem, S., & Zafar, S. (2022). Cyber-security and risky behaviors in a developing country context: A Pakistani perspective. *Security Journal*, 35(4), 1023–1041. <https://doi.org/10.1057/s41284-021-00309-7>
- Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2017). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers & Security*, 42, 165–176. <https://doi.org/10.1016/j.cose.2013.12.003>
- Saunders, M., Lewis, P., & Thornhill, A. (2019). *Research methods for business students* (8th ed.). Pearson Education.
- Higher Education Commission. (2022). *Cybersecurity guidelines for higher education institutions*. [HEC Pakistan Official Website](https://www.hec.gov.pk/cybersecurity-guidelines)
- Ministry of Federal Education and Professional Training. (2023). *Cybersecurity awareness report for educational institutions*. [MoFEPT Pakistan Official Website](https://www.mohe.gov.pk/cybersecurity-awareness-report)
- National Centre for Cyber Security. (2023). *Human factors in cybersecurity initiatives in Pakistan*. NCCS Pakistan Official Website
- Raju, S. (2022). Cybersecurity awareness among university students in digital learning environments. *Journal of Educational Technology Systems*, 51(2), 211–228.