



Analysis of limited Cyber Data in Courts due to Advanced Technology

Sana Azad¹, Qanita Imtiaz²

Hamdard School of Law, Pakistan

*Corresponding Author: qanitaimtiaz@hotmail.com^{1*}

ABSTRACT

Rapid technological advancement has increased cybercrime and created challenges for judicial systems in handling cyber-related cases and digital evidence. This study aims to investigate the factors affecting the use of cyber data and cybersecurity in courts, focusing on technical knowledge, cybersecurity awareness, and technological advancement. This research adopted a quantitative survey design involving 36 adult respondents in Karachi, Pakistan, selected through convenience sampling. Data were collected using a structured questionnaire with a five-point Likert scale and analyzed using SPSS. The regression analysis demonstrated that respondents' perceptions of unauthorized online surveillance were associated with cybersecurity practices ($R^2 = 0.590$). The importance of information security officers ($p = 0.018$) and rejecting application permissions ($p = 0.015$) emerged as significant predictors. Furthermore, rejecting application permissions ($p = 0.021$) and supporting cybersecurity education in university curricula ($p = 0.042$) significantly predicted respondents' willingness to enhance cybersecurity knowledge. These findings emphasize the importance of technical expertise, cybersecurity awareness, and proactive security practices. The study recommends strengthening cybersecurity education, improving digital forensic infrastructure, providing specialized training for legal professionals, and updating cyber laws and policies. However, the small sample size limits the generalizability of these findings to broader populations.

Keywords: cybercrime; cybersecurity awareness; digital evidence; judicial system; Pakistan.

This is an Open Access article distributed under the terms of the Creative Commons Attribution 4.0 International license
<https://creativecommons.org/licenses/by-sa/4.0/>



Article received on 14-08-2026 – Final revised on 20-09-2026 – Approved on 28-10-2026

Introduction

The rapid advancement of technology has made cybercrime more prevalent and challenging to detect. Due to the quick development of technology, there is little examination of cyber data in Pakistani courts, which puts people and organizations at serious risk (Hafiz et al., 2025). These challenges result from the courts' inadequate infrastructure and lack of

awareness of the dangers of cyberspace (Hafiz et al., 2025). But new legislative initiatives, including the Prevention of Electronic Crimes Act (PECA) 2016, show that these problems are being tackled methodically.

Cybersecurity has become a serious problem since cybercriminals are always creating more sophisticated ways to take advantage of flaws in digital systems. It is challenging to investigate crimes and punish offenders because of the public's ignorance, which permits criminals to operate without fear of severe repercussions. One of the most significant duties of law enforcement organizations is investigating and solving crimes (Mofokeng & Aphane, 2022). Evidence from the crime scene, whether digital or physical, must be properly collected and preserved for a crime investigation to be effective.

A crime scene, according to Cyber data, including emails, social media posts, and mobile texts, is now frequently used as evidence in court. However, gathering comprehensive data has become increasingly challenging due to new gadgets and applications. For example, disappearing WhatsApp messages, encrypted chats, and data stored in other countries cannot always be accessed. Reviews of the digital forensics field likewise identify encryption, cloud storage, the proliferation of connected devices, and the growing volume of data as persistent obstacles to the complete acquisition and analysis of digital evidence (Casino et al., 2022).

This creates challenges for judges and lawyers when determining whether the data is authentic and reliable. When the reliability of digital evidence cannot be adequately tested, the fairness of criminal proceedings and the presumption of innocence may be undermined (Stoykova, 2021). Pakistan has laws such as PECA 2016 and the Qanun-e-Shahadat Order to guide the use of electronic evidence, but many gaps still remain. With new technology like encrypted chats and disappearing messages, courts in Pakistan often receive only limited cyber data.

The rapid growth of cyberspace has enabled a wide range of online activities, including communication, recruitment, propaganda, financial transactions, and cyber-attacks, making digital environments increasingly complex and difficult to regulate (Shad, 2019). This growing complexity creates challenges for courts in collecting, analyzing, and interpreting cyber data, particularly in cases involving cybercrime and digital evidence. Computer crimes from embezzlement to cyber terrorism are rising due to the lack of skilled experts, insufficient financial resources, and unclear laws.

Lack of cooperation between agencies and weak law and order further makes it difficult to respond effectively to cyber threats. With more than 35 million people using mobile devices to access the internet, the number of digital offenses is rapidly increasing. By the end of 2025, Pakistan experienced a 35% rise in cybercrime complaints. The main threats were financial fraud and WhatsApp hacking. Authorities now receive an average of 200 complaints daily, highlighting the urgent need for greater technological awareness and capacity building. Many discriminatory practices in cyber-crime cases target women and minority victims, such as women suffering from cyber harassment, who are often blamed in courts (Khan, 2023). Women are particularly vulnerable to online abuse, as 45% of the 3,000 cybercrime incidents reported to the FIA between 2014 and 2015 involved women being targeted through social media.

AI Governance Theory explains how legal institutions adapt to rapidly evolving digital technologies such as artificial intelligence, big data, and automated systems. Contemporary

AI governance scholarship similarly points to a persistent gap between high-level governance principles and the practical mechanisms needed to oversee technology-driven systems (Birkstedt et al., 2023). According to the hypothesis, existing legal frameworks and courts find it more difficult to adequately control and understand digital evidence as technology advances. Large amounts of encrypted data, algorithm-generated logs, and cloud-based records in cybercrime cases present difficulties for judges and investigators who might not have the technological know-how or resources to examine them. Because of this, courts frequently base their rulings on a little amount of cyber evidence. The courts in Pakistan are finding it difficult to keep up with cybercrime. They do not have enough labs for digital evidence or basic forensic instruments (Hafiz et al., 2025).

By stressing the need for updated legal procedures, specialized training, and improved digital forensic infrastructure, the application of AI Governance Theory helps explain the gap between technological innovation and the legal system's capacity to analyze digital evidence. Limited technical knowledge means people don't have enough knowledge about how to use computers, the internet, or other digital tools properly, so they don't know how to protect their online information. Cross-national survey evidence shows that individuals' cybersecurity knowledge is closely related to their level of cyber awareness and to the protective measures they adopt online (Zwilling et al., 2022). This lack of knowledge can make them easier target for Cyber criminals. Prevention of cybercrime depends heavily on the level of society's awareness and education in technology related matters (Hafiz et al., 2025).

Due to their critical role in guaranteeing the proper application of the law and safeguarding individuals' legitimate rights and interests, lawyers may find it difficult to manage cybercrime issues if they lack the necessary technical expertise. To the best of the authors' knowledge, this is among the first studies to provide primary, individual-level survey evidence from adult internet users in Karachi on cybersecurity literacy and digital behaviour and to interpret this evidence in relation to the limited availability of cyber data in Pakistani courts. In this respect, the study complements the predominantly doctrinal and institution-focused literature reviewed above.

Lack of cyber security means not having enough measures to protect computers, networks, and online data from hackers or attacks. This includes weak passwords, outdated software, and poor security practices, which make individuals and organizations vulnerable to hacking, fraud, and other cybercrimes. However, in 2016, the Government of Pakistan passed the Prevention of Electronic Crimes Act (PECA), which still does not cover many of today's cyber threats, such as crimes across borders and other advanced cyber techniques. Cybersecurity in Pakistan is still largely reactive and suffers from poor coordination, weak institutional consistency, and an unsustainable legal framework. People may be encouraged to commit cybercrimes when legal frameworks are permissive; strict laws are necessary to instill fear in potential offenders, so they are aware that there will be repercussions if they commit the crime.

Using digital forensic solutions, such as threat detection and encryption, can increase resistance to cyber threats. Rapid advancement of technology means the fast development and improvement of modern digital tools, systems, and innovations such as the internet, smartphones, and software, which continuously change how people live and work. New tools, devices and software are being created faster than people or laws can fully understand

or control them. Many police departments lack the necessary training and equipment to effectively investigate and prosecute cybercrimes. Research on police investigations in England and Wales likewise shows that the integration of digital forensics into routine casework is constrained by resource pressures, training needs, and growing volumes of digital material (Wilson-Kovacs, 2021). Additionally, jurisdictional challenges make it difficult to handle crimes that cross national borders.

The increase in cybercrime means growing numbers of crimes that are committed using mobile devices, computers, or the internet. These crimes include online fraud, identity theft, hacking, and cyber harassment. Because more people are using computers, the internet, and other digital devices, the number of cybercrime incidents is rising. Time-series evidence from the United Kingdom, for instance, shows that cybercrime and online fraud increased markedly as daily activities shifted online during the COVID-19 pandemic (Kemp et al., 2021). Computer hacking and phishing via email scams have become far more common in recent years. These techniques enable cybercriminals to gain unauthorized access to computer systems, obtain private or sensitive information, and use that information to commit fraud (Siddiqui, 2017). These growing numbers show that more people are being targeted by digital crimes over time.

Several studies have examined cyber law and cybersecurity in Pakistan, although from different angles. Hafiz et al., (2025), combining a literature review with qualitative comparative analysis, found that judges and lawyers frequently lack the technical expertise needed to interpret digital evidence, that PECA 2016 contains vague terms and lacks explicit provisions for emerging offences such as ransomware and deepfake extortion, and that limited forensic resources and case backlogs weaken enforcement. Their analysis, however, is doctrinal and is not grounded in primary survey data.

Bokhari, (2023), one of the few quantitative studies in this field, surveyed 172 managers of banking and IT firms and found that corruption, discrimination, illicit conduct, and legal ambiguity significantly hinder the implementation of cybersecurity laws, whereas expertise and public confidence support it; the study nevertheless reflects organisational rather than individual perspectives. Shad, (2019) assessed Pakistan's cyber threat landscape and the challenges to its readiness. Taken together, these studies concentrate on legislation, institutions, and organisations, and they rarely capture how ordinary internet users' technical knowledge and security practices relate to cybercrime and, ultimately, to the cyber data that reach the courts.

Previous studies on cyber law in Pakistan have mainly focused on the challenges faced by the judiciary in implementing cybersecurity laws and on the legislative gaps and enforcement challenges of PECA. Relatively few studies have examined how limited technical knowledge, lack of proper cybersecurity, and rapid advancement of technology relate to the increase in cybercrime cases from the perspective of the public. The novelty of this study therefore lies in examining these relationships quantitatively based on the perceptions of adult residents of Karachi, and in using AI Governance Theory to explain the gap between technological innovation and the legal system's capacity to analyze digital evidence.

Accordingly, this study aims to examine the relationship between limited technical knowledge, lack of proper cybersecurity, and rapid advancement of technology and the increase in cybercrime cases, based on the perceptions of adult residents of Karachi. Although

the respondents are not judges, lawyers, or court staff, their perceptions are relevant because ordinary internet users are both the most frequent victims of cybercrime and the main producers of the digital traces that may later be presented as cyber evidence. Accordingly, the judicial implications discussed in this article are inferred indirectly from public perceptions rather than from the direct experience of court actors.

The study shows how technology can help the Judiciary handle cyber security issues more quickly and efficiently. The judiciary of Pakistan is implementing reforms to improve efficiency accountability and create a more friendly legal framework (Kasuri et al., 2022). The study helps identify problems that cause delays so courts can deliver justice more quickly and fairly. Despite challenges, Pakistan is working on digital transformation to create a more efficient, transparent and fair legal system through innovation and strong partnership.

Research Method

This section describes the research design, area of study, population, sample, sampling technique, instrument for data collection, administration of the instrument, and method of data analysis.

Research Design

Because it was thought to be suitable for addressing the research questions and accomplishing the study's goals, the study used a quantitative survey research design. Survey research entails gathering information from a chosen sample of respondents to investigate their beliefs, attitudes, experiences, and views on a specific topic. The traits and opinions of the group being studied are then ascertained using the data collected from the respondents. A systematic questionnaire was employed in the current study to gather quantitative information from the participants.

Because it allowed the researcher to get data on public attitudes about cutting-edge technology, cybersecurity literacy, digital behaviours, risk awareness, and the constraints of cyber data in court-related circumstances, the survey design was deemed appropriate. The independent variables of this study are limited technical knowledge, lack of proper cybersecurity, and rapid advancement of technology, while the dependent variable is the increase in cybercrime cases. The relationship between these variables is presented in the theoretical framework in Figure 1.



Figure 1. Theoretical Framework

Based on this, the following hypotheses are developed:

H1: There is a strong relationship between limited technical knowledge and an increase in cyber-crime cases.

H2: There is a strong relationship between lack of proper cyber security and an increase in cyber-crime cases.

H3: There is a strong relationship between rapid advancement of technology and an increase in cyber-crime cases.

Delimitation of the Study

The study was carried out in Pakistan's Karachi, Sindh. Due to time, resource, and respondent access constraints, the research's geographic scope was restricted to Karachi. Adult Karachi residents who utilize, comprehend, or might be impacted by technology, cybersecurity, cyber data, and digital systems in legal or court-related contexts were the study's primary emphasis. Karachi was chosen because it is a significant urban and legal hub where the use and effects of digital technology are pertinent to the study's topic. There were just 36 responses in all for the survey. Therefore, it is not appropriate to instantly extrapolate the results to the entire population of Karachi or Pakistan, as they represent the opinions and impressions of the chosen participants.

Population of the Study

Adult Karachi citizens who were pertinent to the research topic and could offer information on technology, cybersecurity, digital behaviours, and cyber data in legal or court-related contexts made up the study's population. The population was geographically restricted to Karachi for the purposes of this study. The current study did not seek to examine the entire population of Pakistan, even though problems with cutting-edge technology and cyber data may affect people all over the country. Therefore, adult Karachi residents who were reachable by the researcher and ready to take part in the survey were the study's target audience.

Sample of the Population

36 adult respondents who lived in Karachi made up the study's sample. Those who were available and willing to take part in the study were chosen as respondents. The availability and accessibility of respondents within the constraints of time and resources available for the study determined the sample size of 36. The sample size was not established using a probability-based sampling formula or the Krejci and Morgan (1970) sample-size table since the study used a non-probability convenience sampling technique. One of the study's limitations is the very small sample size. As a result, the results should not be regarded as statistically representative of the entire population of Karachi or Pakistan, but rather as reflecting the opinions and perceptions of the chosen respondents.

Sampling Technique

The study's respondents were chosen using a convenience sample technique. Convenience sampling is a non-probability sampling method where participants are chosen based on their availability and willingness to take part. The respondents were chosen from among Karachi's accessible adult population who agreed to fill out the survey. There was no attempt to guaranty that each member of the population had an equal chance of being chosen, and no random selection process was employed. Due to time, resource, and population access constraints, this sample strategy was chosen for the study. Convenience sampling is a non-

probability sampling technique; hence it is not possible to statistically generalize the results to the whole population with a high degree of accuracy.

Instrument for Data Collection

The main tool for gathering data was a structured questionnaire. Closed-ended questions and comments intended to gather quantitative data from the respondents made up the majority of the questionnaire. Cybersecurity literacy, digital behaviour, risk awareness, institutional learning, sophisticated technology, and opinions about the availability and constraints of cyber data in court-related situations were all included in the questionnaire. A five-point Likert scale was used to measure pertinent questionnaire topics, enabling respondents to express how much they agreed or disagreed with the remarks.

Google Forms was used to create the questionnaire, which was then sent via WhatsApp and other online communication platforms to responders who could be reached in Karachi. Respondents were able to easily complete the survey using their computers or mobile devices thanks to the usage of an online questionnaire. Additionally, Google Forms made it easier to electronically gather and arrange the responses for later study.

Validity and reliability of the instrument

By matching the statements and questions to the study's goals and research topics, an attempt was made to guaranty the validity of the questionnaire. Before being distributed, the instrument was examined for consistency, relevance, and clarity. The study's key concepts – cybersecurity literacy, digital behaviour, risk awareness, and attitudes about cyber data and cutting-edge technology in court-related contexts were reflected in the questionnaire items. There was no formal statistical reliability assessment, such as Cronbach's alpha. This is recognized as a study constraint. As a result, care should be taken while interpreting the results. To evaluate the internal consistency of the questionnaire prior to its final administration, future research should include pilot testing and formal reliability analysis, including Cronbach's alpha when appropriate.

Method of Data Collection

After the questionnaire was finalized, data was gathered online using Google Forms. Accessible adult Karachi citizens received the survey link via WhatsApp and other suitable internet communication platforms. The study had 36 completed responses in total. Participants may use their computers or mobile phones to complete the questionnaire, and online data collection offered a practical and effective way to contact respondents. Based on their knowledge and comprehension of cybersecurity, digital technology, and cyber data, the respondents expressed their opinions and perceptions. Google Forms was used to automatically record the responses, which were then arranged for statistical analysis.

The entire data collection method was conducted with ethical issues in mind. Respondents were made aware of the study's purpose prior to filling out the questionnaire, and participation in the study was entirely voluntary. Participants were free to decide whether or not to fill out the questionnaire and were neither coerced nor pressured to participate. The information gathered was used only for academic and research reasons, and the respondents' privacy and confidentiality were maintained.

The presentation and analysis of the results did not purposefully reveal any needless personal information. The results were reported without identifying specific responders. Before gathering data from human subjects, official ethical approval should be acquired if mandated by institutional policy. It should be noted as a research restriction if official ethical approval was not obtained for this study.

Ethical Consideration

The entire data collection method was conducted with ethical issues in mind. Respondents were made aware of the study's purpose prior to filling out the questionnaire, and participation in the study was entirely voluntary. Participants were free to decide whether to fill out the questionnaire and were neither coerced nor pressured to participate. The information gathered was used only for academic and research reasons, and the respondents' privacy and confidentiality were maintained. The presentation and analysis of the results did not purposefully reveal any needless personal information.

The results were reported without identifying specific responders. Before gathering data from human subjects, official ethical approval should be acquired if mandated by institutional policy. It should be noted as a research restriction if official ethical approval was not obtained for this study.

Method of Data Analysis:

The data collected through Google Forms were organised, coded, and analysed using descriptive and limited inferential statistical techniques. The questionnaire included items measured on a five-point Likert scale. Numerical values were assigned to the responses as follows:

Strongly Agree (SA) = 5

Agree (A) = 4

Neutral (N) = 3

Disagree (D) = 2

Strongly Disagree (SD) = 1

Descriptive statistics, including frequencies, percentages, and mean scores, were used to summarise and interpret the responses of the 36 participants and to determine the general level of agreement with each questionnaire item. Where appropriate, an independent-samples t-test was used to examine differences in perceptions between two clearly defined groups, such as respondents with higher technological literacy and respondents with more limited digital exposure, regarding the accessibility and limitations of cyber data in courts. A significance level of 0.05 was used for hypothesis testing. Where the p-value was less than 0.05, the null hypothesis was rejected, indicating a statistically significant difference between the relevant groups.

Where the p-value was equal to or greater than 0.05, there was insufficient evidence to reject the null hypothesis. Multiple regression analysis involving eleven predictors was not considered appropriate for a sample of 36 respondents because the sample size was insufficient to support a reliable regression model of that complexity. Therefore, the analysis focused primarily on descriptive statistics and limited comparisons between relevant groups.

Because of the small sample size and the use of convenience sampling, the findings should be interpreted as exploratory and should not be broadly generalised to the entire population of Karachi or Pakistan.

Methodological Limitation

There are some methodological issues with the study. First, only 36 responders made up the study's comparatively tiny sample. Second, convenience sampling was employed, which means that the respondents were not chosen at random and might not accurately reflect Karachi's total population. Third, the study used self-reported responses, which could be impacted by respondents' unique perspectives, experiences, and expertise. Fourth, no formal statistical reliability tests were performed, such as Cronbach's alpha. Furthermore, the study was restricted to Karachi. As a result, it is not appropriate to instantly extrapolate the results to other cities or the Pakistani populace. Despite these drawbacks, the survey offers insightful preliminary data on attitudes toward cutting-edge technology, cybersecurity, and restrictions connected to cyber data in court-related circumstances.

In summary, the methodology of this study can be outlined as follows. The study was restricted to Karachi, Sindh, Pakistan, and employed a quantitative survey research approach. Adult Karachi citizens who were pertinent to the study's topic made up the population. Convenience sampling was used to choose a sample of 36 respondents. A Google Forms-created questionnaire was used to gather data, and it was disseminated online via WhatsApp and other readily available communication methods. Although rigorous statistical reliability testing was not carried out, the questionnaire was examined for relevance and clarity.

Result and Discussion

Data Presentation and Analysis

This section presents the analysis of limited cyber data in courts due to advanced technology. The primary goal is to examine how limited technical knowledge, lack of proper cybersecurity, and rapid technological advancement relate to the increase in cybercrime cases and, by extension, to the use and handling of cyber data in judicial proceedings. The study is based on responses from 36 respondents belonging to Karachi. All responses were recorded through a structured questionnaire using a five-point Likert scale, where participants indicated their level of agreement with different statements.

The data was later processed and analyzed using SPSS. Because a few items were left unanswered, the number of valid responses ranges from 34 to 36 across items, and 35 complete cases were available for the regression analysis. As stated in the Method section, multiple regression with eleven predictors is not well suited to a sample of this size. The three regression models generated during the initial SPSS analysis are nevertheless reported below for transparency, but they are interpreted strictly as exploratory, with particular attention to the Adjusted R Square values and the overall F-tests.

Demographic Information of Respondents

Gender

Figure 2 shows the gender distribution of respondents. Females make up 77.1% of the sample, while males represent 22.9%. This indicates that female participants were more in number compared to male participants in the survey.

35 responses

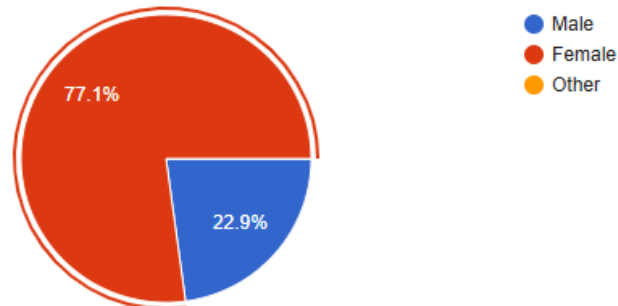


Figure 2. Gender Distribution of Respondents (n = 35)

Source: Primary survey data (Google Forms), processed by the authors.

Age

Figure 3 shows the age distribution of the respondents. The respondents were concentrated in the two youngest age groups: those aged less than 20 years and those aged 21 to 30 years each accounted for 47.2% (n = 17) of the responses. Only one respondent (2.8%) belonged to each of the 31 to 40 and 41 to 50 years age groups, and no respondent was aged 51 years or above.

Age

36 responses

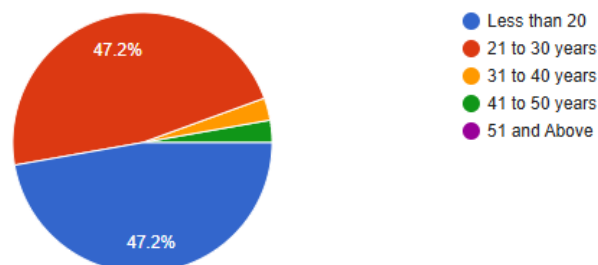


Figure 3. Age Distribution of Respondents (n = 36)

Source: Primary survey data (Google Forms), processed by the authors.

Household Income

Figure 4 shows the household income level of the respondents. Most participants belong to the income group of 105,000 above representing 34.3% of the total responses. The income group of less than 25,000 makes up 28.6%, while 85,000–105,000 represents 25.7% of the respondents. Very few participants belong to the income groups of 25,000–45,000, 45,000–65,000 and 65,000–85,000, as shown by the smallest portion of the chart.

35 responses

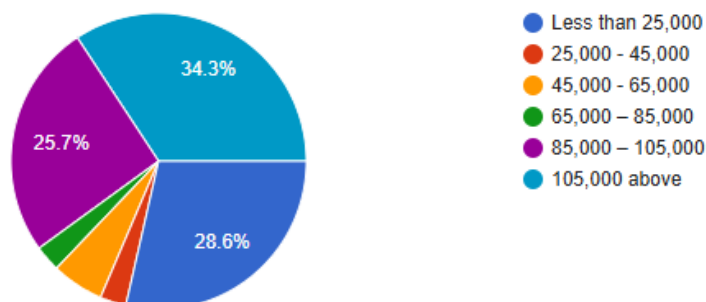


Figure 4. Household Income Level of Respondents (n = 35)

Source: Primary survey data (Google Forms), processed by the authors.

Qualification

Figure 5 shows the educational qualifications of the participants. Most of the respondents belong to the bachelor's level, with 61.1% responses. Participants from Intermediate make up 22.2%, while Matric or less Students are 11.1% of the total respondents. Very few participants belong to the master's and PhD, as shown by the smallest portion of the chart.

36 responses

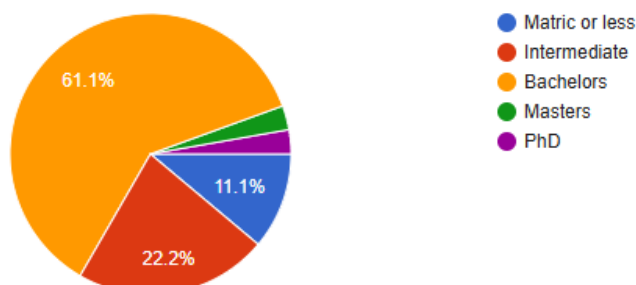


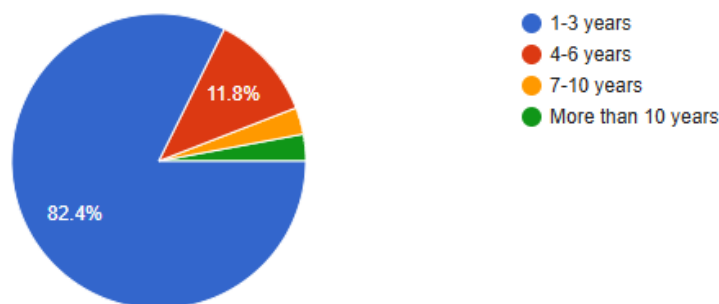
Figure 5. Educational Qualification of Respondents (n = 36)

Source: Primary survey data (Google Forms), processed by the authors.

Work Experience

Figure 6 shows the working experience of the respondents. Most participants have 1-3 years of working experience, representing 82.4% of the total responses. Respondents with 4-6 years of experience make up 11.8%. Very few participants belong to the 7-10 years and more than 10 years, as shown by the smallest portion of the chart.

34 responses

**Figure 6.** Work Experience of Respondents (n = 34)

Source: Primary survey data (Google Forms), processed by the authors.

Exploratory Regression Analysis

Model Summary

Table 1. Model Summary of Regression Model 1

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.768 ^a	.590	.394	.888

Source: SPSS output, processed by the authors.

Intrepretation

Regression analysis was used to look at what influences respondents' perceptions of being watched online without their permission. A significant correlation between the independent factors and the dependent variable was indicated by the model's R value of 0.768. The model's predictors account for 59% of the variation in the dependent variable, according to the R Square value of 0.590. After taking into consideration the number of predictors, the model explains around 39.4% of the variance in the dependent variable, according to the Adjusted R Square value of 0.394.

In general, the model's ability to predict respondents' opinions about internet surveillance is moderate. The overall model was statistically significant, $F(11, 23) = 3.01$, $p = 0.012$. However, the substantial gap between the R Square (0.590) and the Adjusted R Square (0.394) indicates that part of the explained variance stems from the large number of predictors relative to the number of cases (eleven predictors for 35 cases, roughly three cases per predictor). This pattern is a typical sign of overfitting; hence, the Adjusted R Square provides the more realistic estimate of explanatory power, and the model should be regarded as exploratory.

Table 2. Coefficients of Regression Model 1 (Dependent Variable: Perceived Online Observation without Consent)

Model	Variables	B	Std. Error	Beta	t	Sig.
1	(Constant)	-2.257	1.521	—	-1.483	.152

When you receive an email from an unfamiliar sender? Do you open it?	-.180	.138	.221	-	.205
Do you know what Two-Factor Authentication (2FA) is and do you use it?	.088	.151	.093	.584	.565
In your opinion, is it important that academic institutions should have an information security officer?	.731	.287	.422	2.542	.018
Do you ever reject app permission?	.646	.244	.442	2.644	.015
Do you use debit or credit cards at an outdoor payment machine?	-.075	.213	.079	-.351	.729
Do you use a harder-to-guess password to access your bank account than to access your social networking accounts?	-.095	.234	.089	-.406	.689
Do you consider yourself knowledgeable about cybersecurity?	.049	.155	.061	.319	.753
Do you think to add cybersecurity awareness in university curriculum?	.080	.299	.064	.267	.792
Do you use the same passwords for both social networks such as Facebook, Twitter, and your email account?	.106	.177	.120	.601	.554
Do you shop/purchase items advertised on social networks or your private email?	.119	.223	.117	.534	.599
Do you know what is the difference between using HTTP and HTTPS?	-.040	.146	.048	-.274	.786

a. Dependent Variable: Do you have reason to believe that you are being observed online without your consent

Source: SPSS output, processed by the authors.

Interpretation

Only two predictors were statistically significant at the 5% significance level among the variables in the model, according to the coefficients analysis. The dependent variable ($B = 0.731$, $p = 0.018$) was significantly positively impacted by the variable "In your opinion, is it important that academic institutions should have an information security officer?" This suggests that respondents who thought the presence of an information security officer was important were more likely to think they were being watched online without their consent.

In a similar vein, it was discovered that the variable "Do you ever reject app permissions?" was a significant positive predictor ($B = 0.646$, $p = 0.015$), indicating that those who refuse needless app permissions are more likely to be aware of or concerned about online monitoring. The remaining factors were not statistically significant predictors of the dependent variable since their p-values were higher than 0.05. These results imply that views toward institutional cybersecurity measures and cybersecurity awareness are associated with respondents' sensitivity to online surveillance. Because only 35 cases were available for eleven predictors, these associations should be regarded as preliminary.

Table 4. Model Summary of Regression Model 2

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	0.707 ^a	0.500	0.261	0.863

Source: SPSS output, processed by the authors.

Interpretation

The purpose of the regression study was to investigate how the independent and dependent variables were related. A moderate to strong association between the predictors and the dependent variable was shown by the model's R value of 0.707. The independent variables in the model account for half of the variation in the dependent variable, as indicated by the R Square value of 0.500. After accounting for the number of predictors, the model explains around 26.1% of the variance in the dependent variable, according to the Adjusted R Square value of 0.261.

The average prediction error is reflected in the Standard Error of the Estimate (0.863), which indicates the mean deviation of the observed data from the regression line. The model's overall explanatory power is moderate. However, the overall F-test was not statistically significant at the 5% level, $F(11, 23) = 2.09$, $p = 0.066$, which means that the predictors as a set do not reliably explain the dependent variable. Together with the sharp decline from R Square (0.500) to Adjusted R Square (0.261), this result indicates overfitting and suggests that Model 2 should be interpreted with particular caution.

Table 5. Coefficients of Regression Model 2 (Dependent Variable: Rejection of Mobile App Permission Requests)

Model	Variable	B	Std. Error	Beta	t	Sig.
1	(Constant)	0.201	1.479	—	-0.136	0.893
	When you receive an email from an unfamiliar sender? Do you open it?	-0.054	0.134	-0.075	-0.403	0.691
	Do you know what Two-Factor Authentication 2FA is and do you use it	0.066	0.147	0.079	0.451	0.656
	In your opinion is it important that academic institutions should have an information security officer?	0.226	0.280	0.148	0.809	0.427
	Do you ever reject app permission?	0.596	0.238	0.463	2.509	0.020
	Do you use debit or credit cards at an outdoor payment machine?	0.149	0.207	0.179	0.720	0.479
	Do you use a harder to guess password to access your bank account than to access your social networking accounts	-0.077	0.228	-0.082	-0.339	0.737
	Do you consider yourself knowledgeable about cybersecurity	-0.260	0.150	-0.363	-1.728	0.097
	Do you think to add a cybersecurity awareness in university curriculum?	0.265	0.291	0.241	0.913	0.371

Do you use the same passwords for both social networks such as Facebook, Twitter, and your email account?	0.240	0.172	0.309	1.399	0.175
Do you shop/purchase items advertised on social networks or your private email?	-0.175	0.217	-0.194	-0.805	0.429
Do you know what is the difference between using HTTP and HTTPS?	0.008	0.142	0.011	0.055	0.957

Dependent Variable: Have you ever rejected a mobile app request for accessing your contacts, camera or location?

Source: SPSS output, processed by the authors.

Interpretation

Each independent variable's unique impact on the dependent variable is displayed in the coefficients table. Only one of the predictors was shown to be statistically significant at the 5% level. The dependent variable was significantly positively predicted by the variable "Do you ever decline app permission?" ($B = 0.596$, $p = 0.020$). This suggests that respondents are more likely to exhibit greater levels of the outcome variable linked to cybersecurity perception/awareness (i.e., having rejected a mobile app request to access contacts, camera, or location) if they actively refuse app permissions.

The other factors were not statistically significant predictors because their p-values were all higher than 0.05. These include actions like opening emails from unknown senders, understanding HTTP vs. HTTPS, using two-factor authentication, perceptions of information security officers, using payment machines, password practices, cybersecurity knowledge, awareness of cybersecurity curricula, using the same passwords across accounts, and online shopping. Overall, the findings indicate that while other cybersecurity-related awareness and behavior factors do not have a significant direct influence in this model, only app permission behavior is statistically significant in predicting the dependent variable.

This result should, however, be interpreted with caution because the predictor ("Do you ever reject app permission?") and the dependent variable ("Have you ever rejected a mobile app request for accessing your contacts, camera or location?") measure almost the same behaviour. The significant coefficient therefore largely reflects the consistency of respondents' answers rather than a substantive explanatory relationship and, given that the overall model was not significant, it does not provide evidence for the study's hypotheses.

Table 6. Model Summary of Regression Model 3

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	0.724 ^a	0.524	0.296	0.898

Source: SPSS output, processed by the authors.

Interpretation

The factors impacting respondents' desire to learn more about cybersecurity were investigated using regression analysis. A significant correlation between the independent factors and the dependent variable was indicated by the model's R value of 0.724. The predictors in the model account for 52.4% of the variation in the dependent variable, according

to the R Square value of 0.524. After accounting for the number of predictors, the model explains around 29.6% of the variance, according to the Adjusted R Square value of 0.296.

The model's average prediction error is represented by the Standard Error of the Estimate (0.898). The model exhibits a moderate degree of explanatory power overall. The overall model was statistically significant at the 5% level, $F(11, 23) = 2.30$, $p = 0.044$, although the decline from R Square (0.524) to Adjusted R Square (0.296) again points to overfitting arising from the small number of cases relative to predictors.

Table 7. Coefficients of Regression Model 3 (Dependent Variable: Desire to Learn More about Cybersecurity)

Model	Variable	B	Std.Error	Beta	t	Sig.
1	(Constant)	-1.520	1.539	—	-0.988	0.334
	When you receive an email from an unfamiliar sender? Do you open it?	-0.089	0.139	-0.117	-0.641	0.528
	Do you know what Two-Factor Authentication 2FA is and do you use it	0.164	0.153	0.183	1.069	0.296
	In your opinion is it important that academic institutions should have an information security officer?	0.349	0.291	0.214	1.199	0.243
	Do you ever reject app permission?	0.614	0.247	0.447	2.483	0.021
	Do you use debit or credit cards at an outdoor payment machine?	0.247	0.216	0.278	1.147	0.263
	Do you use a harder to guess password to access your bank account than to access your social networking accounts	-0.419	0.237	-0.418	-1.768	0.090
	Do you consider yourself knowledgeable about cybersecurity	-0.055	0.157	-0.071	-0.349	0.731
	Do you think to add a cybersecurity awareness in university curriculum?	0.651	0.302	0.554	2.154	0.042
	Do you use the same passwords for both social networks such as Facebook, Twitter, and your email account?	0.029	0.179	0.035	0.163	0.872
	Do you shop/purchase items advertised on social networks or your private email?	-0.178	0.226	-0.185	-0.788	0.439

Model	Variable	B	Std.Error	Beta	t	Sig.
	Do you know what is the difference between using HTTP and HTTPS?	0.000	0.147	0.000	0.002	0.998

a. Dependent Variable: Do you desire to learn more about cybersecurity?

Source: SPSS output, processed by the authors.

Interpretation

Each independent variable's unique effect on respondents' desire to learn more about cybersecurity is displayed in the coefficients table. Two factors were determined to be statistically significant at the 5% level among all the predictors. "Do you ever decline app permission?" was a significant positive predictor ($B = 0.614$, $p = 0.021$). This suggests that respondents are more likely to be motivated to learn more about cybersecurity if they actively refuse needless app permissions. In a similar vein, the variable "Do you think to add a cybersecurity awareness in university curriculum?" was also statistically significant ($B = 0.651$, $p = 0.042$), indicating that respondents are more likely to express interest in learning more about cybersecurity if they support the inclusion of cybersecurity awareness in academic curricula.

The other factors were not statistically significant predictors because their p-values were all higher than 0.05. Email behavior, two-factor authentication knowledge, perceptions of information security officers, payment security practices, password usage, general cybersecurity knowledge, and comprehension of HTTP vs. HTTPS are some of these. Overall, the findings indicate that academic interest in cybersecurity education and proactive security behavior (like refusing app permissions) are the main factors influencing respondents' desire to learn more about cybersecurity; other factors do not appear to have a significant direct impact in this model.

Hypothesis Testing

The research hypothesis was tested to determine the relationship between variables. The hypothesis is:

The purpose of hypothesis testing was to examine the relationship between independent variables, namely limited technical knowledge, lack of proper cybersecurity, and rapid advancement of technology, with the increase in cyber-crime cases. The findings indicate that limited technical knowledge significantly contributes to the rise in cyber-crime cases, as individuals and institutions with inadequate technical expertise face greater difficulties in identifying, preventing, and responding to cyber threats.

The lack of proper cybersecurity measures was found to be associated with an increase in cyber-crime incidents, as weak security systems create opportunities for cybercriminal activities. Furthermore, the results reveal that the rapid advancement of technology has a strong relationship with the increase in cyber-crime cases, as technological developments continuously introduce new digital methods of cyberattacks. Therefore, based on the findings of the study, all three hypotheses (H1, H2, and H3) are accepted, indicating that limited technical knowledge, lack of proper cybersecurity, and rapid technological advancement are significantly contributing to the increase in cyber-crime cases.

Discussion of Findings

The findings of the study reveal that improving the understanding, protection, and management of cyber data requires technical knowledge and cybersecurity awareness. Comparable survey studies support this pattern: university students in Saudi Arabia displayed only an average level of cybersecurity awareness and frequently failed to translate their knowledge into precautions such as avoiding emails from unknown senders and password reuse (Alharbi & Tassaddiq, 2021), while a national survey of 1,230 internet users found that about one-third had no knowledge of phishing and that most cybercrime victims did not report the incident (Alzubaidi, 2021), which in turn limits the cyber data that can reach investigators and courts.

The findings also show that insufficient cybersecurity safeguards and limited technical expertise create significant challenges in the handling and verification of digital evidence. Experimental evidence shows that digital forensic examiners analysing the same evidence file can reach inconsistent observations and conclusions, and that contextual information can bias their analysis (Sunde & Dror, 2021). The adoption of generative AI tools in forensic examination may offer efficiency gains, but it also raises new concerns about the accuracy and verifiability of results that are ultimately presented as evidence (Scanlon et al., 2023).

These results are in line with earlier research that emphasized the widening gap between technology advancements and the ability of legal institutions to adapt (Rehman, 2025). At the same time, artificial intelligence is increasingly applied to user authentication, network situation awareness, and the detection of abnormal behaviour and traffic, although scholars stress that human judgement must remain part of AI-driven security decisions (Zhang et al., 2022). The study also shows that enhancing cyber laws, specialist training, and technology infrastructure could improve courts' capacity to manage cyber-related cases and digital evidence more effectively. Grounding digital evidence rules in the right to a fair trial has been proposed as a conceptual framework for ensuring that such evidence remains reliable and open to meaningful challenge by the parties (Stoykova, 2023).

The data was analyzed using SPSS. The results showed that hypotheses were supported, which means that the expected relationships were strong enough to be considered statistically significant. The study found that better digital awareness and stronger cyber security practices can improve the management of cyber data in judicial proceeding. The significance of support for cybersecurity education in university curricula is consistent with a study of 517 university students in Kyrgyzstan, which found weak cybersecurity awareness and recommended formal cybersecurity education to reduce victimisation (Erendor & Yildirim, 2022).

Similarly, a comparative study of 1,652 university students and working graduates in China reported awareness and behaviour scores that were mostly below adequate levels, with working graduates scoring lowest in areas such as email use and incident reporting (Hong et al., 2023). The relevance of cautious email behaviour is further underlined by a systematic review showing that phishing attacks succeed largely by exploiting human factors, including users' limited knowledge and awareness (Desolda et al., 2022). Nonetheless, because the present findings rest on self-reported perceptions, they should be read in light of evidence that most studies of cybersecurity-related behaviour rely on self-report surveys rather than observation of actual behaviour (Kannelønning & Katsikas, 2023).

Conclusions

This study examined the challenges associated with the limited use of cyber data in courts due to advanced technology, focusing on cybersecurity awareness, technical knowledge, and increasing cybercrime cases. The findings reveal that technical expertise and cybersecurity awareness are important for understanding, protecting, and managing cyber data. Insufficient cybersecurity safeguards and limited technical knowledge create challenges in handling and verifying digital evidence. The results also highlight the importance of cybersecurity education and proactive security practices in improving awareness of digital threats. Therefore, improving digital education, providing specialized training for legal professionals, strengthening digital forensic infrastructure, and updating cyber laws and policies are essential recommendations. However, the small sample size and convenience sampling limit the generalizability of the findings. Future research should involve larger samples and examine institutional and legal factors.

Acknowledgement

The authors would like to express their sincere gratitude to all respondents who participated in this study and contributed valuable information regarding cybersecurity awareness, technical knowledge, and digital evidence. Appreciation is also extended to Hamdard School of Law for its academic support. The authors acknowledge everyone who contributed to the completion of this research.

References

- Alharbi, T., & Tassaddiq, A. (2021). Assessment of Cybersecurity Awareness among Students of Majmaah University. *Big Data and Cognitive Computing*, 5(2), 23. <https://doi.org/10.3390/bdcc5020023>
- Alzubaidi, A. (2021). Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia. *Heliyon*, 7(1), e06016. <https://doi.org/10.1016/j.heliyon.2021.e06016>
- Birkstedt, T., Minkinen, M., Tandon, A., & Mäntymäki, M. (2023). AI governance: themes, knowledge gaps and future agendas. *Internet Research*, 33(7), 133–167. <https://doi.org/10.1108/INTR-01-2022-0042>
- Bokhari, S. (2023). A quantitative study on the factors influencing implementation of cybersecurity laws and regulations in Pakistan. *Mdpi.ComSAA BokhariSocial Sciences*, 2023•*mdpi.Com*. <https://www.mdpi.com/2076-0760/12/11/629>
- Casino, F., Dasaklis, T. K., Spathoulas, G. P., Anagnostopoulos, M., Ghosal, A., Borocz, I., Solanas, A., Conti, M., & Patsakis, C. (2022). Research Trends, Challenges, and Emerging Topics in Digital Forensics: A Review of Reviews. *IEEE Access*, 10, 25464–25493. <https://doi.org/10.1109/ACCESS.2022.3154059>
- Desolda, G., Ferro, L. S., Marrella, A., Catarci, T., & Costabile, M. F. (2022). Human Factors in Phishing Attacks: A Systematic Literature Review. *ACM Computing Surveys*, 54(8), 1–35. <https://doi.org/10.1145/3469886>
- Erendor, M. E., & Yildirim, M. (2022). Cybersecurity Awareness in Online Education: A Case Study Analysis. *IEEE Access*, 10, 52319–52335. <https://doi.org/10.1109/ACCESS.2022.3171829>
- Hafiz Abdul Rehman Saleem, Ali Bukhtiar, Babar Zaheer, & Muhammad Asad Ullah Farooq.

- (2025). Challenges Faced by the Judiciary in Implementing Cybersecurity Laws in Pakistan. *The Critical Review of Social Sciences Studies*, 3(1), 1052–1066. <https://doi.org/10.59075/1wyx0v30>
- Hong, W. C. H., Chi, C., Liu, J., Zhang, Y., Lei, V. N.-L., & Xu, X. (2023). The influence of social education level on cybersecurity awareness and behaviour: a comparative study of university students and working graduates. *Education and Information Technologies*, 28(1), 439–470. <https://doi.org/10.1007/s10639-022-11121-5>
- Kannelønning, K., & Katsikas, S. K. (2023). A systematic literature review of how cybersecurity-related behavior has been assessed. *Information & Computer Security*, 31(4), 463–477. <https://doi.org/10.1108/ICS-08-2022-0139>
- Kasuri, M., Abbas, S. (2022). Imbalance Criminal Justice System of Pakistan: Joined Up Working is the Way Forward. *Gssrjournal.Com* MR Kasuri, S Abbas, G Ahmed *Global Social Sciences Review*, 2022•*gssrjournal.Com*.
- Kemp, S., Buil-Gil, D., Moneva, A., Miró-Llinares, F., & Díaz-Castaño, N. (2021). Empty Streets, Busy Internet: A Time-Series Analysis of Cybercrime and Fraud Trends During COVID-19. *Journal of Contemporary Criminal Justice*, 37(4), 480–501. <https://doi.org/10.1177/10439862211027986>
- Mofokeng, J., & Aphane, M. (2022). Evaluating knowledge management capabilities during crime scene processing in the detective service. *Papers.Ssrn.Com* JT Mofokeng, MP Aphane *OIDA International Journal of Sustainable Development*, 2022•*papers.Ssrn.Com*.
- Scanlon, M., Breiting, F., Hargreaves, C., Hilgert, J.-N., & Sheppard, J. (2023). ChatGPT for digital forensic investigation: The good, the bad, and the unknown. *Forensic Science International: Digital Investigation*, 46, 301609. <https://doi.org/10.1016/j.fsidi.2023.301609>
- Shad, M. (2019). Cyber threat landscape and readiness challenge of Pakistan. *JSTORMR Shad Strategic Studies*, 2019•*JSTOR*.
- Stoykova, R. (2021). Digital evidence: Unaddressed threats to fairness and the presumption of innocence. *Computer Law & Security Review*, 42, 105575. <https://doi.org/10.1016/j.clsr.2021.105575>
- Stoykova, R. (2023). The right to a fair trial as a conceptual framework for digital evidence rules in criminal investigations. *Computer Law & Security Review*, 49, 105801. <https://doi.org/10.1016/j.clsr.2023.105801>
- Sunde, N., & Dror, I. E. (2021). A hierarchy of expert performance (HEP) applied to digital forensics: Reliability and biasability in digital forensics decision making. *Forensic Science International: Digital Investigation*, 37, 301175. <https://doi.org/10.1016/j.fsidi.2021.301175>
- Wilson-Kovacs, D. (2021). Digital media investigators: challenges and opportunities in the use of digital forensics in police investigations in England and Wales. *Policing: An International Journal*, 44(4), 669–682. <https://doi.org/10.1108/PIJPSM-02-2021-0019>
- Zhang, Z., Ning, H., Shi, F., Farha, F., Xu, Y., Xu, J., Zhang, F., & Choo, K.-K. R. (2022). Artificial intelligence in cyber security: research advances, challenges, and opportunities. *Artificial Intelligence Review*, 55(2), 1029–1053. <https://doi.org/10.1007/s10462-021-09976-0>
- Zwilling, M., Klien, G., Lesjak, D., Wiecheteck, 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>

