P-ISSN 2708-6453	Pakistan Languages and Humanities Review	Jan-Feb 2026, Vol. 10, No. 1
O-ISSN 2708-6461	https://doi.org/10.47205/plhr.2026(10-I)08	[70-82]

Pakistan Languages and Humanities Review
www.plhr.org.pk

RESEARCH PAPER

Cybersecurity in Pakistan: Public Opinion and the Effectiveness of Government Response

[1]Neha Arif, [2]Rehmat Arif and [3]Arooj Fatima

1. MS Scholar, Department of Politics & IR, GC Women University Sialkot, Punjab, Pakistan
2. MS Scholar, Department of Politics & IR, GC Women University Sialkot, Punjab, Pakistan
3. MS Scholar, Department of Politics & IR, GC Women University Sialkot, Punjab, Pakistan

***Corresponding Author** nehaarif06@gmail.com

ABSTRACT

In the digitalization world, Pakistan faces challenges due to the expansion of online social media and financial frauds. Cyberattacks such as malware, phishing, and hacking make cybersecurity awareness necessary among the citizens and at the national level. This study examines the public opinion on cybersecurity awareness and government initiatives. A quantitative research approach was adopted using an online survey that was designed to collect data from 400 participants. The results show that cyber security awareness, knowledge of government initiatives, and cyber law remain limited. Many citizens use security practices, but citizens' behavior—clicking suspicious links—faces cyberattacks. The study further shows that experiences of cybercrimes negatively impact public trust. The report concludes that strengthening institutional collaboration, public awareness campaigns, and law enforcement are essential to improving cybersecurity governance and rebuilding public confidence in Pakistan.

KEYWORDS Cybersecurity, Public Opinion, Cyber Threats, Government Working, Cyber Laws and Institution

Introduction

Cyber security is rapidly becoming a major concern in the digitalized world. In contemporary times, increases in cyberattacks also increased, such as malware, phishing, hacking, ransomware attacks, denial of service (DOS), etc. Cybersecurity is a mechanism in which "cyber," related to the network and computer, and "security" relate to the planning that is used to prevent any illegal activity that is done by unauthorized users. Cybersecurity is needed to protect the military maps, government offices, and nuclear or arms data. According to a 2025 report, approximately 142,000 cybercrimes face Pakistan. In 2025 conflict between India and Pakistan is not only limited to military action; it also includes the digital war as cyber war.

In Pakistan the growing use of technologies brought systems online, such as personal information, economy, election, and defense, which are serious causes for both citizens and institutions. Cybersecurity not only protects personal information, but it also protects the military, global communication, and election results at national and international levels. Due to weak security, hackers leak data breaches and use it illegally for terrorism and national threats. Public mistrust in state institutions. Due to these challenges, cybersecurity is extremely important (Kaifa, et al. 2025).

Public opinion is vitally important for evaluating government initiatives, citizens' personal experiences, and awareness toward cybersecurity. Prevention of the Electronic

Crime Act (PECA) 2016: Many citizens are unaware of this act. This study analyzes public opinion on cybersecurity in Pakistan by examining public awareness, personal experience with cyber threats, and perception of government initiatives and also provides recommendations for protecting cybersecurity.

Literature Review

Landscape of cybersecurity in Pakistan

Previous studies have shown that the growth of digitalization in Pakistan increases the cyber threats. As citizens and industries and businesses rely on online platforms, the cyber threats such as malware, phishing, hacking, and ransomware have grown rapidly. Due to the low rank of Pakistan on the global cybersecurity index, the government introduced the Prevention of the Electronic Crimes Act (PECA) in 2016. This act aims to protect aware citizens from cybercrimes. Pakistan faces several challenges, such as technical expertise and public awareness, which has hidden the cybersecurity measures. Moreover, the data security is further complicated by regional and global threats, including aggressive state-planned cyber warfare (Shad, 2021).

Cyber security threats in Pakistan

In digitalization world Pakistan is 87 million network access that the serious challenged due to growing of cyber-attacks. Digital advertising and online internet presence rely on public trust, but the country's low cyber security infrastructure and economic-disparities increase vulnerability. Addressing these challenges require Education, legislative action, and technology experts. Moreover, in order to promote an encoding environment and opportunity advantage indeed invest in strong cybersecurity systems in the Sustainable Development Goals of the United Nations (Mehmood, 2025).

According to the UN Charter, Pakistan's technology role is ranked in the world. Accessibility grows from 6.3% in 2005 to 17.8% in 2016, with 25.32% mobile internet as part of the broader (51 million users) and 26.46% (54 million users). The Cybersecurity Global Index ranked Pakistan 67th due to the rise of malware and cybersecurity risk. Implementing measures such as PECA 2016 for strengthening national security is challenging due to the growing vulnerability of cyberattacks. Cyberspace is more involved in global war (Khan , Raza , & Naseer , 2021).

Digital media not only circulate information but also play a significant role in shaping public opinion. Media coverage may be biased, but other times it encourages youth to participation, rises, awareness, and influences public perspective (Asghar, Cheema, & Muzaffar, 2025). Previous studies examine the growing cybersecurity awareness through education, where traditional cultural variables are influenced by behavior. Effective strategies needed include theoretical seminars and social media meetings. Additionally, public awareness, understanding, and training address cyber threats (Amjad, Naeem , Zaffar, Choo, & Zaffar, 20116).

Government Policies and Implementation

Pakistan enacted several laws & regulations that address cybersecurity and telecommunication. The Pakistan Telecommunication Reorganization Act in 1996 was empowered for financial transactions. The Electronic Transaction Act 2002 was encouraged for e-governance due to the legal record being electronic. The Prevention of Electronic Crimes Act 2016 deals with cybercrimes and aims to protect personal privacy. Regardless,

these measures lack cyber security knowledge, technology expertise, and growing cyberattack vulnerability. The Pakistan government introduced The National Security Policy (2021) for cyberspace protection (Kashan, et al., 2022).

The National Telecom & Information Technology Security Board (NTISB) of Pakistan demands the implementation of policies to shield the government and organizations from cyberattacks after the breach of private information by the US National Security Agency (NSA). Currently, Pakistan lacks extensive cybercrime laws and vulnerability. Professional experts suggest establishing a Cyber Crime Unit (CCU) and developing laws that control these issues, evidenced by a Tanzanian delegation's recommendation after comparable difficulties (Awan & Memon , 2016).

As technology advances and new cyber threats emerge, cyber legislation and cyber-security laws have evolved differently in each country. The difficulties creating effective cyber laws because of social media bullying and human fundamental rights. The Electronic Transaction Ordinance (2002) and the Prevention of Electronic Crimes Act (2016) are important legislative attempts to address cyber vulnerability. For comparison, Canada and Australia places a strong structure framework for data protection to national (Watto, Islam, Hussain, & Shahab, 2024).

Pakistan Cyber Trends

Cybercrimes in Pakistan have a wide range of identity theft, cyberterrorism, child pornography (sexual act content), and cyber harassment. Identity theft, which involves the unauthorized user stealing credit card data and Social Security numbers, results in large financial fraud. The detention strategy monitors tracking sensitive access requests and examining bank records. Child pornography, which is the illegal sharing of sexual content that involves kids. Cyberbullying uses social media to harass people; common methods include information manipulation and verbal abuse. The tracking process is similar to that of cyberterrorism, which is harmful (Ibrahim , Nnamani , & Okosun, 2021).

Pakistan's national security handles multiple challenges, including terrorism, political instability, and defense war as regional conflict. According to the global terrorism index, Pakistan ranked 4th with several groups such as Tehreek-e-Taliban. Current or future threats are internal, such as terrorism and lack of technological expertise; external threats are espionage, such as spies and military maps. The collective collaboration is significant to protect Pakistan from cybercrime vulnerability (Rehman, Ishaque, & Sayed, 2025).

Cybercrimes in Pakistan are growing rapidly, impacting both local and global trends. Over 45% of internet access is victim of phishing cases. Women and minority persons are mostly affected by cyber harassment. Misinformation creates social unrest. In 2023, the Bank of Punjab had a computer data breach in which hackers gained access to over 500,000 individuals' personal information and stole PKR 2.3 billion. A critical cybersecurity weakness was exposed by this event, which resulted in a 15% decline in digital banking operations, according to cybersecurity examinations. Another incidence involves blackmail using social media to target people, especially women, with over 1,200 victims in one case in Lahore (Khan, 2025).

Pakistan landscape is complicated by lacking the ICT-dependent system, security measures, and geopolitical situation. Institutions like NADRA (National Database and Registration Authority) collect citizen data and share it with other sectors to move citizen online management. To properly manage and explore its cyber environment, Pakistan

needs effective legislation and a collaborative approach sharing, in response to protect citizens from threats (Baig , 2023). Digital media not only share information but also play a significant role in shaping public opinion. Media coverage may be biased, but other times it encourages youth to participation, rise, awareness, and shape public perspective.

Socioeconomic Barrier and Digital Illiteracy Gap

The gap between digital socioeconomic and disparity digital illiteracy in Pakistan, especially in rural areas where basic knowledge of awareness is limited. These cybercrimes vulnerability make restrict of digital services. Different programs like Raast aim to use safe payment systems and build sustainable socioeconomic programs. However, Pakistan's vision intends to improve technology expertise and literacy rate for betterment. Effective security measures having faith in Sustainable Development Goals of the United Nations. Pakistan's approach to creating a safe and friendly digital platform. (Mehmood , 2025) According to the computer emergency response team (CERT), big initiatives and coordination among multiple industries will boost cybersecurity in modern times. This regulation step demonstrates how the government safeguards emerging materials and improves responses to data breaches; both are vital to the security of Pakistan (Masudi & Mustafa , 2023).

In Pakistan internet access grew from 0.1 to 10.6% in 2009. As growing internet access grows cyber threats… For example, poor digital skills can lead to cyber threats like phishing and data breaches and can even cause problems like ATM ransomware and the WannaCry abuse incident. Although most people know about cybersecurity, the socioeconomic gap between awareness and practices makes the illiteracy rate increase on digital platforms. For better results, all sectors work together, like institutions, lawmakers, and trainers, to overcome these issues (Parvez , 2025).

Although previous studies documented the types of cybercrimes, cybersecurity threats, and government initiatives, fewer studied the awareness of cybersecurity among common citizens. This study aims to quantitatively analyze the awareness, experience, and public perspective on cybersecurity and cybercrimes.

Hypotheses

H1: There is a significant relationship between citizens' cybersecurity awareness and their opinion of government initiatives to address cyber threats in Pakistan.

H2: Citizens who have experienced cyber threats show lower levels of trust in government cybersecurity performance.

H3: Fear of cyberattacks significantly influences public trust and confidence in digital technologies and cybersecurity governance.

Theoretical Framework

Institutional Trust Theory by Putnam (1993, 2000) and Mishler & Rose (2001). Many scholars working on cyber security but this theory related with this study that based on public awareness, governance, and technology.

Institutional Trust Theory

This theory is given by Putnam (1993, 2000) and Mishler & Rose (2001) on how public opinion is shaped by government initiatives. In this study examining how public

opinions and analyses of policies, particularly throughout the area of cybersecurity in Pakistan, are influenced by their integrity governmental bodies, this research uses the Institutional Trust Theory. According to the theory, construing political decisions as productive, inclusive, and trustful is closely linked with high trust in organizations; on the other hand, it is engagement associated with design that shapes public opinion despite the level of care for the real or laws. Citizens opinions on trust level and the government's abilities to influence and recognize cyberwar fare are highly affected by their involvement in data security. People who are more trusting realize that cybersecurity practices are important, while people who are less trusting easily have concerns about the government's abilities, also in scenarios where enough systems are in the corner. The majority's viewpoint is influenced by media and news. This study analyses how institutional activities affect the cybersecurity by judging the public opinion on government initiatives (ROSE, 2001).

Conceptual Framework

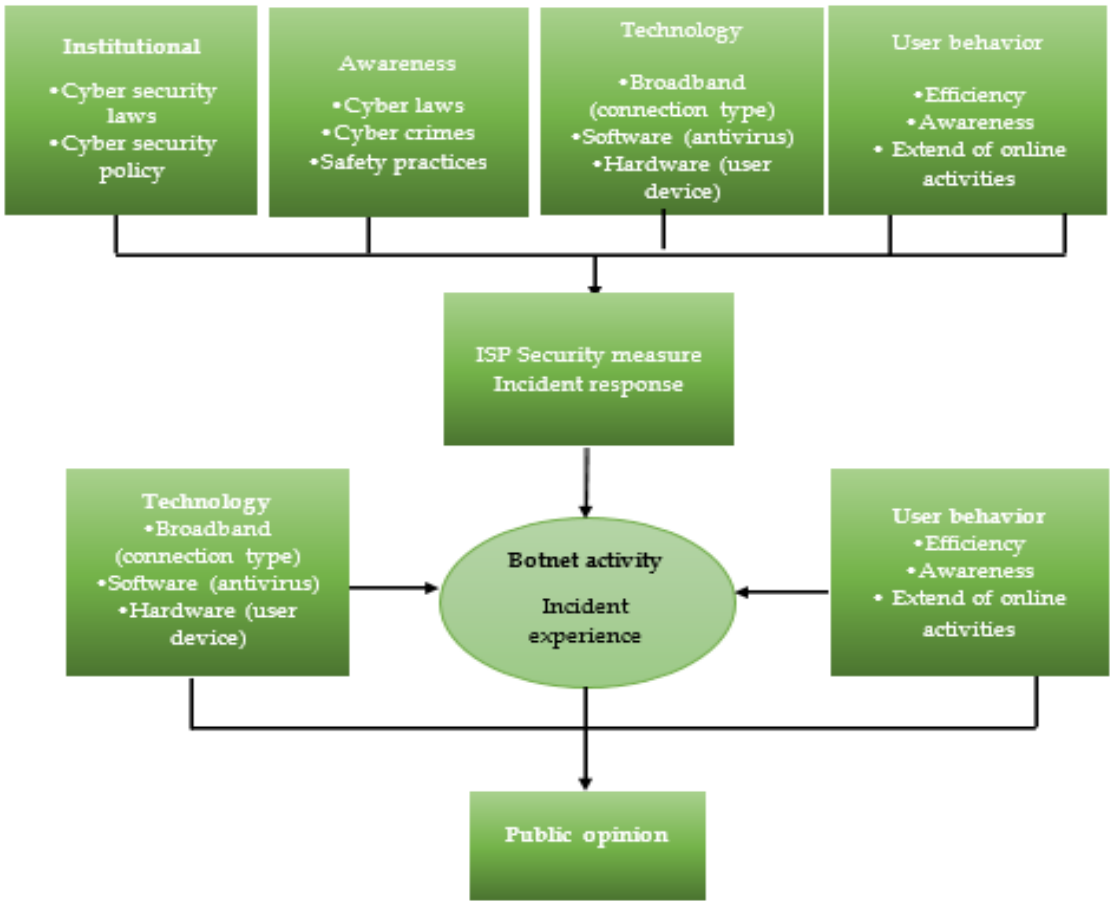

Figure 1 Conceptual Framework

Material and Methods

Research design

This research is descriptive in nature and adopts a quantitative method that examines public opinion on cybersecurity and government working to protect citizens from cybercrimes. It aimed to understand the citizen opinion, awareness, and experience regarding cybersecurity. This article was conducted using both primary sources, such as surveys, and secondary sources, such as articles and reports.

Population

Since the digitalization era, most young people use internet access and are the best demographic for this study. This study targets the population of common citizens from diverse educational backgrounds.

Sample size

The Cochran formula was used, and the minimum sample size is 400 generalized common citizens.

Procedure of Selecting Sample

This study used quantitative research that was based on a questionnaire in Google Forms. Therefore, it is descriptive in nature and targets the common citizens with diverse sociodemographic backgrounds. Moreover, the population targets consist of 400 participants.

Instrument of Study

The data was collected through a questionnaire consisting of 16 statements. The five points of the Likert scale were used to measure response, allowing the statistical analysis measure. For the nature of the questionnaire, the Likert scale was selected as SA (Strongly Agree) = 5, Agree = 4, Neutral = 3, Disagree = 2, and SD (Strongly Disagree) = 1.

Ethical consideration

Ethical considerations: participants are informed of the research purpose, and their response is voluntary. Their personal information was not collected or approved by an expert.

Delimitation

The delimitation of this study is that the response was collected only from those who use internet access. Therefore, only target the common citizens and exclude the technical experts and lawmakers. This study is quantitative-based and targets the 400 population and also consults with experts.

Reliability and Validity of Tools

The study used a questionnaire that ensured both the reliability and validity of the standardized Likert scale that allowed consistent measurement of participants. The validity of this study ensures that the questionnaire is made based on literature and also improved by expert and related theoretical frameworks added to strengthen the validity. The coefficient value is collected by MS Excel and SPSS.

Table 1
Gender

Gender	Frequency	%
Female	364	91
Male	34	8.5%
Transgender	0	0

Table 1 shows that 91% (346) females participated and 8.5% (34) male citizens participated while no transgender individual participated. This shows that majority of participants are females.

Table 2
Education

Education	Frequency	%
Matric	42	10.5
Intermediate	30	7.5
Undergraduate	199	49.75
Graduate	87	21.75
Post-Graduate	42	10.5

Table 2 indicate that 42 (10.5%) citizens from Matric and 30 (7.5%) from Intermediate, 199 (49.75%) from Undergraduate and 87 (21.75%) Graduate citizens 42 (10.5%) from Post-graduate common citizen participate.

Table 3
Occupation

Occupation	Frequency	%
Student	229	57.25
Employed	92	23
Unemployed	55	13.75
Other	24	6

Table 3 demonstrate 299 (57.25%) are students and 92 (23%) are employed citizens, 55 (13.75%) are unemployed and 24 (6%) are others citizens that participate. The majority population are student citizens.

Table 4
Meaning of cybersecurity

Item no.	Statement	Level	F	%	Mean score
1	I know the meaning of the term "cybersecurity."	Strongly Agree	176	44%	3.81
		Agree	49	12.25%	
		Neutral	130	32.5%	
		Disagree	14	3.5%	
		Strongly Disagree	31	7.75 %	

Table 4 show that 176 (44%) citizens are Strongly Agree and 49 (12.25%) citizens are Agree, 130 (32.5%) are neutral citizens and 14 (3.5%) are Disagree and 31 (7.75%) are Strongly Disagree citizens to know the meaning of term cybersecurity.

Table 5
Online threats such as hacking, malware, phishing

Item no.	Statement	Level	F	%	Mean score
2	I know the online threats like phishing, hacking, and malware.	Strongly Agree	161	40.25%	3.84
		Agree	70	17.5%	
		Neutral	128	32%	
		Disagree	29	7.25%	
		Strongly Disagrees	12	3%	

Table 5 depict that 161 (40.25%) are Strongly Agree and 70 (17.5%) citizens are Agree, 128 (32%) Neutral citizens and 29 (7.25%) citizens are Disagree or 12 (3%) are Strongly Disagree to this statement.

Table 6
Personal information

Item no.	Statement	Level	F	%	Mean score
3	I know how personal information is misused.	Strongly Agree	173	43.25	3.91
		Agree	69	17.25%	
		Neutral	118	29.5%	
		Disagree	32	8%	
		Strongly Disagree	8	2%	

Table 6 demonstrate that 173 (43.25%) are Strongly Agree and 69 (17.25%) citizens are Agree, 118 (29.5%) Neutral citizens and 32 (8%) citizens are Disagree or 8 (2%) are Strongly Disagree to this statement.

Table 7
Online links checking

Item no.	Statement	Level	F	%	Mean score
4	I carefully check online link before clicking on them	Strongly Agree	95	23.75%	2.96
		Disagree	43	10.75%	
		Neutral	131	32.75%	
		Agree	15	3.75%	
		Strongly Disagree	116	29%	

Table 18 indicate that 95 (23.75%) are Strongly Agree and 43 (10.75%) citizens are Agree, 131 (32.75%) Neutral citizens and 15 (3.75%) citizens are Disagree or 116 (29%) are Strongly Disagree to this statement.

Table 8
Awareness among cyber laws

Item no.	Statement	Level	F	%	Mean score
5	I'm aware of the cyber laws and security institutions.	Strongly Agree	120	30%	3.16
		Disagree	38	9.5%	
		Neutral	126	31.5%	
		Agree	20	5%	
		Strongly Disagree	96	30%	

Table 8 depict that 120 (30%) are Strongly Agree and 38 (9.5%) citizens are Agree, 126 (31.5%) Neutral citizens and 20 (5%) citizens are Disagree or 96 (30%) are Strongly Disagree to this statement.

Table 9
Experience toward Suspicious message, calls

Item no.	Statement	Level	F	%	Mean score
6	I received suspicious messages, calls, and emails.	Strongly Agree	136	34%	3.00
		Agree	28	7%	
		Neutral	72	18%	
		Disagree	30	7.5%	
		Strongly Disagree	134	33.5%	

Table 9 shows that 136 (34%) are Strongly Agree and 28 (7%) citizens are Agree, 72 (8%) Neutral citizens and 30 (7.5%) citizens are Disagree or 134 (33.5%) are Strongly Disagree to this statement.

Table 10
Experience toward NADRA (ID) Information stolen

Item no.	Statement	Level	F	%	Mean score
7	I experienced personal information from NADRA (ID) being stolen.	Strongly Agree	112	28%	2.61
		Agree	20	5%	
		Neutral	56	14%	
		Disagree	26	6.5%	
		Strongly Disagree	186	46.5%	

Table 10 shows that 112 (28%) are Strongly Agree and 20 (5%) citizens are Agree, 56 (14%) Neutral citizens and 26 (6.5%) citizens are Disagree or 26 (6.5%) are Strongly Disagree to this statement.

Table 11
Experience toward online fraud

Item no.	Statement	Level	F	%	Mean score

8	I have experience with online financial fraud.	Strongly Agree	144	36%	2.92
		Agree	23	5.75%	
		Neutral	46	11.5%	
		Disagree	34	8.5%	
		Strongly Disagree	153	38.25%	

Table 11 depict that 144 (36%) are Strongly Agree and 23 (5.75%) citizens are Agree, 46 (11.5%) Neutral citizens and 34 (8.5%) citizens are Disagree or 153 (38.25%) are Strongly Disagree to this statement.

Table 12
Hacking social accounts

Item no.	Statement	Level	F	%	Mean score
9	I have experienced unauthorized access to my social accounts.	Strongly Agree	95	23.75%	2.69
		Agree	35	8.75%	
		Neutral	79	17.75%	
		Disagree	36	9%	
		Strongly Disagree	155	38.75%	

Table 12 demonstrate that 95 (23.75%) are Strongly Agree and 35 (8.75%) citizens are Agree, 79 (17.75%) Neutral citizens and 36 (9%) citizens are Disagree or 155 (38.75%) are Strongly Disagree to this statement.

Table 13
Security practices using 2AF (2 Factor-Authentication)

Item no.	Statement	Level	F	%	Mean score
10	I use two-factor authentication for social accounts.	Strongly Agree	155	38.75%	3.12
		Agree	39	9.75%	
		Neutral	31	7.75%	
		Disagree	50	12.5%	
		Strongly Disagree	125	31.25%	

Table 10 indicate that 155 (38.75%) are Strongly Agree and 39 (9.75%) citizens are Agree, 31 (7.75%) Neutral citizens and 50 (12.5%) citizens are Disagree or 125 (31.25%) are Strongly Disagree to this statement.

Table 14
Mixed password used for security concern

Item no.	Statement	Level	F	%	Mean score
11	I used strong or mixed passwords for my accounts.	Strongly Agree	172	43%	3.41
		Agree	48	12%	
		Neutral	59	14.75%	
		Disagree	15	3.75 %	
		Strongly Disagree	106	26.5%	

Table 14 depict that 172 (43%) are Strongly Agree and 48 (12%) citizens are Agree, 59 (14.75%) Neutral citizens and 15 (3.75%) citizens are Disagree or 106 (26.5%) are Strongly Disagree to this statement.

Table 15
Log-out accounts in public places

Item no.	Statement	Level	F	%	Mean score
12	I log out of accounts after using public or shared device	Strongly Agree	164	41%	3.64
		Agree	85	21.25%	
		Neutral	25	6.25%	
		Disagree	95	23.75%	
		Strongly Disagree	31	7.75%	

Table 15 depict that 164 (41%) are Strongly Agree and 85 (21.25%) citizens are Agree, 25 (6.25%) Neutral citizens and 95 (23.75%) citizens are Disagree or 31 (7.75%) are Strongly Disagree to this statement.

Table 16
Update social accounts for security practices

Item no.	Statement	Level	F	%	Mean score
13	I update my account for security concerns.	Strongly Agree	169	42.25%	3.83
		Agree	55	13.75%	
		Neutral	130	32.5%	
		Disagree	31	7.75%	
		Strongly Disagree	15	3.75%	

Table 18 shows that 169 (42.75%) are Strongly Agree and 55 (13.75%) citizens are Agree, 130 (32.5%) Neutral citizens and 31 (7.75%) citizens are Disagree or 15 (3.75%) are Strongly Disagree to this statement.

Table 17
Opinion toward lack of cyber awareness

Item no.	Statement	Level	F	%	Mean score
14	Lack of cyber awareness increases the risk of cybercrimes.	Strongly Disagree	194	49.25%	2.88
		Agree	5	1.25%	
		Neutral	47	11.75%	
		Disagree	5	1.25%	
		Strongly disagree	12	3%	

Table 18 depict that 194 (49.25%) are Strongly Agree and 5 (1.25%) citizens are Agree, 47 (11.75%) Neutral citizens and 5 (1.25%) citizens are Disagree or 12 (3%) are Strongly Disagree to this statement.

Table 18
Cyber-attack fear affect public

Item no.	Statement	Level	F	%	Mean score
15	Fear of cyberattack affects the public trust and their mental well-being.	Strongly Agree	194	48.5 %	4.19
		Agree	143	35.75%	
		Neutral	28	7%	
		Disagree	17	4.25%	
		Strongly disagree	18	4.5%	

Table 18 demonstrate that 194 (48.5%) are Strongly Agree and 143 (35.75%) citizens are Agree, 28 (7%) Neutral citizens and 17 (4.25%) citizens are Disagree or 18 (4.5%) are Strongly Disagree to this statement.

Table 19
Government imitative steps to improve cybersecurity

Item no.	Statement	Level	F	%	Mean score
16	The government organization takes active steps to monitor and improve cybersecurity.	Strongly Agree	55	13.75%	3.45
		Agree	67	16.75%	
		Neutral	113	28.25%	
		Disagree	35	8.75 %	
		Strongly disagree	130	32.5%	

Table 19 indicate 130 (32.5%) are Strongly Agree and 67 (16.75%) citizens are agree, 113 (28.5%) neutral citizens and 35 (8.75%) citizens are disagree or 55 (13.75%) are strongly disagree to this statement.

Table 20
Statement wise mean score

Statement no.	Mean score	Statement no.	Mean score

15	4.19	10	3.12
3	3.91	6	3.00
2	3.84		
13	3.83	4	2.96
1	3.81	8	2.92
		14	2.88
12	3.64	9	2.69
16	3.45	7	2.61
11	3.41		
5	3.16		
Average mean scores of 16 statement = 3.338			

Table 20 show that statement 15 to 1 **(M= 4**.19 to 3.81) indicate the high level of acceptance and statement 3 to 6 (**M=**3.91 to 3.00) indicate the moderate level and statement 4 to 7 **(M=**2.96 to 2.61) indicate the low level of acceptance. The total acceptance of mean score is 3.338.

Testing of Hypotheses

Table 21
Summary of Z test Hypothesis

Hypothesis	Mean Score	Z-value	Significance	Decision
H1	3.52	10.4	$p < 0.05$	Accepted
H2	2.805	3.9	$p < 0.05$	Accepted
H3	3.535	10.7	$p < 0.05$	Accepted

Z-test analysis

H1:

For this hypothesis, Statement 16 (government initiatives) was analyzed. Mean = 3.52 Test value = 3 Sample size = 400 The calculated Z-value exceeded the critical value of ±1.96.

The Z test result show that the government initiative mean score =3.52 which is higher than the TV (test value) = 3. The statistically calculated the Z-test is significant $p<0.05$. However, the H1 is accepted. This test show that the citizens positively prescribe government initiative and believe these initiatives improve the awareness in citizens.

H2:

This hypothesis was examined using experience-based statements (Statements 6–9), which showed mean scores ranging from 2.61 to 3.00, indicating relatively low trust and confidence. he calculated Z-values were statistically significant at $p < 0.05$.

This result show that experience of cyber security mean score =2.08 which is lower than the TV. =3. The statistically collected Z test is significant as $p<0.05$. H2 hypothesis is accepted. This result indicate that experience of cyber threats linked with low level of trust on government cybersecurity performance.

H3:

This hypothesis was tested using Statement 15. Mean = 4.19 Test value = 3 Sample size = 400. The calculated Z-value was much higher than the critical value.

This result indicates that the fear of cyberattacks Mean value =4.19 which is higher than the TV=3 value. The statistically calculated Z test at $p<0.05$. H3 is accepted. The result show that fear of cyber-attacks significantly impacts public trust and well-being.

Conclusion

This study used quantitative research to properly assess the public's view of data security at the state level. Due to increased press coverage and internet awareness, it was discovered that such public views cyber security as a critical importance. Even though the government is involved through its cybersecurity, there is still an acknowledged lack of confidence in performance, specifically with respect to clarity, cyber law enforcement, and regulatory execution. The results show that having cyber defense rules alone is incomplete; mutual understanding and efficient implementation are essential. The research identifies the inconsistencies between public performance and actual or state-level performance, indicating that improving institutional frameworks, responsiveness, and public confidence is critical to successful digital governance that provides lawmakers with insightful information.

Recommendations and Policy Implications

Building strong cyber defense laws to handle emerging issues and discourage cyberterrorism is one recommendation to improve governance and boost trust of the people. Planning to put an intense focus on awareness, the government should launch the national cyber policy, having efficient training and resources, and making sure government organizations are necessary to respond to cybersecurity incidents. Increasing public education and information campaigns on cyber threats vulnerability. To tried and trusted, increase openness and communication on cybersecurity protection. The government should launch a data security policy. Using and attempting to cut technology to improve data security and digitization. Promoting public participation in decision-making for realization and validity. By putting these policies into practice, government efficiency may be brought into line with public desires, creating a sustainable online environment.

References

Amjad, H. A., Naeem, U., Zaffar, M. A., Choo, K.-K. R., & Zaffar, M. Z. (2016, June). Improving security awareness in the government sector. *Proceedings of the 17th International Digital Government Research Conference on Digital Government Research*, 1-8.

Awan, J., & Memon, S. (2016). Threats of cyber security and challenges for Pakistan. *International Conference on Cyber Warfare and Security: ICCWS-2016 Boston US*, 425-429.

Asghar, N., Cheema, A, T., & Muzaffar, M. (2025). The Impact of media coverage on political behavior among Pakistani students: A case study of GC Women University Sialkot. *Journal of Development and Social Sciences, 6*(2), 266-279.

Baig, Y. J. (2023). Implementation of cyber security in corporate sector of Pakistan. *International Journal of Advanced Engineering, Management and Science, 9*(10), 1-9.

Ibrahim, S., Nnamani, D. I., & Okosun, O. (2021). Types of cybercrime and approaches to detection. *Journal of Computer Engineering (IOSR-JCE), 23*(5), 24-26.

Kaifa, U., Yaseen, Z. & Muzaffar, M. (2025). A thematic analysis of Pakistan's cybersecurity policies, regulations and implications, *Journal of Climate and Community Development, 4*(1), 39-54.

Kashan, A. H., Mehmood, A., Khan, S. u., Aziz, T., Orakzai, J. K., & Islam, D. M. (2022). Implementation strategies of cybersecurity. *Journal of public policy, 2*(4), 183-218.

Khan, A. U. (2025). Cyber crime in Pakistan: Trends, Challenges, and Legal Responses. *Advance Social Science Archive Journal, 4*(1), 1358-1366.

Khan, M. F., Raza, D. A., & Naseer, D. N. (2021). Cybersecurity and challenges faced by Pakistan. *Pak. Journal of Int'L Affairs, 4*(4), 265-881.

Masudi, D. J., & Mustafa, N. (2023). Cyber security and data privacy law in Pakistan: protection information and privacy in the digital age. *Pak. Journal of Int'L Affairs, 2*(3),

Mehmood, M. (2025). The role of cyber security in promoting digital inclusion: a case study of Pakistan. *Annals of Human and Social Sciences, 6*(1), 35-44.

Parvez, M. W. (2025). *The impact of digital illiteracy on cybersecurit vulnerability: a demographic study in Pakistan*. UNIVERSITY OF JYVÄSKYLÄ .

Rehman, D. Z., Ishaque, D. W., & Sayed, M. H. (2025). Emerging dynamics and national security of Pakistan:challenges and strategies. *Research Consortium Archive, 3*(1), 228

ROSE, W. M. (2001). What are the origins of political trust?: Testing institutional and cultural theories in post-communist Societies. - *Comparative Political Studies - COMP POLIT STUD, 34*(1), 30-62.

Shad, M. R. (2021). Cyber threat landscape and readiness challenge of Pakistan. *Strategic Studies, 39*(1), 1-19.

Watto, O. M., Islam, M., Hussain, S. A., & Shahab, M. (2024). Cyber law and cyber security policies in Pakistan: A comparative study with USA, Canada and Australia. *Pakistan J Humanit Soc Sc, 12*(1), 271-277.