Journal of Research in Economics and Finance Management
ISSN (Print): 2959- 099X ISSN (Online): 2959-1007
Volume 5, Issue 1, Page 65-84, June 30, 2026

CYBERSECURITY THREAT AWARENESS, PERCEIVED CYBERSECURITY RISK, AND STOCK MARKET PARTICIPATION INTENTION: THE ROLE OF INVESTOR CONFIDENCE AMONG RETAIL INVESTORS IN PAKISTAN

Mubasir Qadir[1]
Former Professor
Jinnah Sindh Medical University, Karachi, Pakistan

Shariq Mubashir[2]
Professor
S.M. Law College, Karachi, Pakistan

ABSTRACT

Today, retail investors trade shares on their mobile devices and online brokerage accounts, putting their money and personal information at risk from phishing, account takeover, and data breaches. But little is known about how investors' own understanding of these threats influences their willingness to remain in, or to join, the stock market. This study is based on the theory of planned behavior and the protection motivation theory to explore the relationship between cybersecurity threat awareness and investor confidence, as well as between perceived cybersecurity risk and stock market participation intention. A cross-sectional survey was conducted with 400 individual investors in Pakistan using a 20-item, five-point Likert instrument. The internal consistency (Cronbach's α) of all four constructs was good to excellent (Cronbach's α = .861 to .897, overall α = .914). Pearson correlation analysis revealed the positive relationships between threat awareness and investor confidence (r = .52) and intention (r = .49), while perceived cybersecurity risk was negatively related to investor confidence (r = −.46) and intention (r = −.42). Investor confidence was most highly correlated with participation intention (r = .61) while awareness was negatively associated with perceived risk (r = −.31) and both were significant at $p < .01$. The results indicate that informed investors are more, not less, willing to invest, and that perceived cyber risk lowers confidence and willingness to invest. It is, therefore, time for regulators, exchanges and brokers to consider cyber-awareness education and visible security assurance as integral to the development of the market, not a purely IT matter. The study is one of the first investor-level studies of perceptions of cyber risk in an emerging South Asian market.

The study findings suggest that the theory of planned behavior (TPB) explains investor confidence in the stock market and their participation in the market by incorporating the concepts of cybersecurity threat awareness, perceived cybersecurity risk, and value of the stock market.

INTRODUCTION

Trust is the foundation of stock markets. For an investor who deposits money with a broker, the exchange and a series of electronic platforms, there is a level of trust that the money will be available the next day, and that the rules will be fairly enforced. A lack of such trust can account for the reluctance of many households—even high-income households—to participate in equities at all, as demonstrated by Guiso et al.

This work is licensed under a Creative Commons Attribution 4.0 International License.

(2008). The object of that trust has moved silently in 10 years. Investors no longer work with a person on the trading floor; they work with the applications, passwords, one-time codes and servers that they will never see. This means that the question of the safety of the market is now accompanied by the question of security.

The question has become real with cyber incidents. The literature on event studies has consistently reported that the market value of firms decreases when a security breach becomes public (Campbell et al., 2003; Cavusoglu et al., 2004), and a meta-analysis of 63 studies confirms that the market value of firms declines significantly on average after security breach announcements (Ebrahimi & Eshghi, 2022). The effects of the breaches are not temporary either: Ali et al. (2021) reported abnormal returns of approximately −15% to −18% in the year following a breach announcement, while Kamiya et al. (2021) demonstrated that successful breaches were correlated with a lasting reputational impact and changes in firm risk policy. Florackis et al. (2023) also demonstrated that the cross-section of daily stock returns reflects the firm's cybersecurity risk. From a systemic perspective, the International Monetary Fund (IMF, 2024) has reported that cyber events in financial services have more than doubled over the past few years, and are now a legitimate risk to macrofinancial stability.

Most of the evidence is, however, external, in the form of prices and volumes of markets. Much less is known about what goes on in the investor's mind. There is wide variation in the amount of information investors have regarding phishing, malware, and account fraud, as well as in how much they fear such scams. Someone who understands what the source of the breach is and how to protect against it can feel more in control and therefore more confident. Someone who feels threatened but isn't aware of what to do may retreat. There is a potential for these two reactions to act in opposing ways: first, informed awareness, and second, diffuse perceived risk.

Pakistan is a rewarding place in which to research these issues. The percentage of retail participation in the Pakistan Stock Exchange is still low compared to the population, digitally onboarded investors have grown rapidly, and awareness about online fraud among the public has become commonplace. In a market like this, any cost to the new or existing investor is an actual cost of capital. This study thus explores whether there is a relationship between cybersecurity threat awareness and perceived cybersecurity risk with investor confidence and intention to participate in the stock market among retail investors in Pakistan or not, and the strength of the relationship between investor confidence and intention.

Problem Statement

There are a number of reasons why stock markets are not widely used in emerging economies, and some of them can be attributed to behavioral influences, including trust, literacy and confidence (Balloch et al., 2015; Georgarakos & Pasini, 2011; van Rooij et al., 2011). With the rise of online trading, cybersecurity is a fresh source of perceived risk for the average investor. However, the majority of the literature on cyber risk and markets focuses on firm-level event studies of price reactions to breach announcements (Cavusoglu et al., 2004; Förderer & Schuetz, 2022; Rosati et al., 2017). These studies inform us that markets react but not why individual investors will choose to remain, enter or exit.

ISSN (Print): 2959- 099X ISSN (Online): 2959-1007
Volume 5, Issue 1, Page 65-84, June 30, 2026

Simultaneously, the literature on information security behavior has focused on raising awareness and assessing threats primarily for employees and technology users (Bulgurcu et al., 2010; Ifinedo, 2012; Liang & Xue, 2009), but not investors. Research on the adoption of online trading has involved perceived risk and trust (Lee, 2009) but not much has been done to distinguish between the cyber-specific risk and general financial risk, or compare it to investors' actual awareness of cyber risk. A gap thus exists: currently, there is limited evidence of the relationship between investor-level cyber threat awareness and cyber risk perception and no evidence from South Asia to support the link between investor-level cyber threat awareness and investor confidence and participation. Regulators and brokerage firms in markets such as Pakistan need to know if cyber-awareness campaigns would draw in investors or dissuade them from investing, but they cannot without such evidence.

Study Objectives

The overall objective of this research is to investigate the relationship between the investors' perceptions of cybersecurity and their confidence and intentions to engage in the stock market. The specific objectives are:

- To explore the relationship between cybersecurity threat awareness and investor confidence.
- To look at the correlation between cybersecurity risk perception and investor confidence.
- To examine the relationships of cybersecurity threat awareness and perceived cybersecurity risk with stock market participation intention.
- To analyse the relationship between investor confidence and stock market participation intention.
- To investigate the relationship between cybersecurity threat awareness and perceived cybersecurity risk.
- To provide input to regulators, exchanges, and brokerage firms regarding the need for investor participation in digital trading.

LITERATURE REVIEW

The Stock Market and Cyber Incidents

The first market data regarding cybersecurity were derived from event studies of breach announcements. Campbell et al. (2003) reported that the negative market reactions to breaches of unauthorized access to confidential data were significant, while the market reaction to other breaches was not. Cavusoglu et al. (2004) found that the market value of companies that suffered a breach dropped by approximately 2.1% in the first two days following the announcement. However, in their sample, Kannan et al. (2007) did not obtain negative abnormal returns. Subsequent research provided some explanations for this inconsistency. Förderer and Schuetz (2022) demonstrated that announcements of breaches are made on busy news days, which makes market

reactions more muted, and Ebrahimi and Eshghi (2022) conducted a meta-analysis of the literature to determine how breach type, timing, country, and firm size influence the magnitude of the market response.

The impacts go beyond prices, too. Rosati et al. (2017) reported higher bid–ask spreads and trading volume during the breach announcement days, which is consistent with the idea of breaches causing information asymmetry. Kamiya et al. (2021) found that the attacks have negative abnormal returns and negatively impacted shareholder value, which consequently spurs a corresponding tightening of risk management by firms, while Ali et al. (2021) reported that for up to 12 months following an attack, firms had negative abnormal returns with an increase in their equity risk, and these effects were explicitly observed as a loss of investor confidence. Florackis et al. (2023) took it one step further and created a measure of cybersecurity risk at the firm level, using annual reports to assess the risk, and found that more exposed firms earn a risk premium. Collectively, the literature demonstrates that investors are interested in cyber risk. What it does not tell us is how individual investors understand that risk and how those understandings influence their choices to invest.

Cybersecurity Threat Awareness

Cybersecurity threat awareness is the understanding that a person has of the nature and forms of cyber threats (such as phishing, malware, identity theft, and account takeover) as well as the steps that can be taken to defend against them. Awareness has been considered an important antecedent to protective behavior in the information systems literature. Bulgurcu et al. (2010) determined that IS awareness influences the beliefs regarding the usefulness and cost of compliance, and then the intention to comply with the security policies. Liang and Xue (2009) suggested that people try to avoid technology threats by considering the threat and coping capabilities, and Boss et al. (2015) demonstrated that the combination of threat appraisal and coping capabilities can enhance the motivation to engage in protective action.

The same might apply to investors. The investor who understands how phishing works and how to secure an account is better able to determine if a broker's platform is secure, and how to take individual steps. This feeling of control can help promote confidence and decrease uncertainty. In Taiwan, Lee (2009) found that trust and perceived benefits promoted the adoption, and perceived risk did the opposite, indicating that knowledge that increases trust and decreases risk should help achieve participation.

Perceived Cybersecurity Risk

The concept of perceived risk has existed for a long time in the field of consumer research. According to Bauer (1960), consumer behaviour is a risk-taking behaviour, where the consumer acts under uncertainty in situations where he cannot control the outcomes he is taking. Later, Featherman and Pavlou (2003) even broke perceived risk into different dimensions such as financial risk, privacy risk, and performance risk, and demonstrated that the perceptions of these risks diminish the likelihood of adopting the services. According to Slovic (1987), the risks that are unknown, invisible and difficult to control are considered highly risky, and cyber threats are all of these. Prospect theory also suggests that individuals are more sensitive

ISSN (Print): 2959- 099X ISSN (Online): 2959-1007
Volume 5, Issue 1, Page 65-84, June 30, 2026

to losses than to similar gains (Kahneman & Tversky, 1979), meaning that a small risk of losing money in a fraud could be a huge factor when considering investing.

According to this study, the subjective risk perceived by an investor of his/her money, personally identifiable information, or account being lost due to cyber events related to trading online is perceived cybersecurity risk. Both Pavlou (2003) and Kim et al. (2008) concluded that perceived risk negatively impacts intention to transact online, in part, through the influence of perceived trust. In particular, Kim et al. (2008) demonstrated that trust and perceived risk are closely tied to each other—trust reduces perceived risk, and perceived risk reduces the willingness to transact. The results indicate that investors' intention to participate in the stock market should be negatively correlated with perceived cybersecurity risk and investors' confidence.

Investor Confidence and Stock Market Participation

Investor confidence, as defined herein, means the investor's trust that the market, its intermediaries, and its electronic infrastructure are sufficiently reliable, fair and secure to ensure the security of his or her investment. It is closely related to trust, defined by Mayer et al. (1995) as being willing to be vulnerable to another party because of the party's ability, benevolence and integrity. Guiso et al. (2008) demonstrated that less trusting people are less likely to purchase stocks and do not buy as many stocks when they do. Similarly, using European data, Georgarakos and Pasini (2011) showed that general trust and trust in financial advice both positively affect participation, while Balloch et al. (2015) found that stock market literacy and trust both stand alone in predicting stock ownership.

The evidence from emerging markets is congruent. Even the core factors of the theory of planned behavior were not as well correlated with investors' intention to participate in the stock market as was trust in financial institutions during the COVID-19 period, according to Adil et al. (2023). Van Rooij et al. (2011) demonstrated that financial education increases participation, in part because financial education makes investors less uncomfortable with risk. Of course, confidence can turn into overconfidence (Barber & Odean, 2001), but in the participation literature a reasonable degree of confidence in the market is a prerequisite for entering the market.

Research Gap

From this review, three gaps are identified. First, cyber-risk research has been conducted at the firm level and price level, and perceptions of investors have not yet been investigated. Secondly, security awareness and threat appraisals have been studied in the context of a workforce or technology users, and not investors. Third, no studies have been conducted that simultaneously analyzed cyber-specific awareness, cyber-specific risk, and confidence in participation and/or online trading. Data from South Asian markets is in particular very limited. The present study, thus, tries to fill these gaps by testing an investor-level model in the context of Pakistan.

THEORETICAL FRAMEWORK

Theory of Planned Behavior

According to the theory of planned behavior (TPB) (Ajzen, 1991), intention is the most proximal determinant of behavior and intention is determined by attitudes toward the behavior, subjective norms, and perceived behavioral control. The theory has been extensively used in investment and online trading decisions (Adil et al., 2023; Lee, 2009). The outcome of the present study is the stock market participation intention. The theory situates investor confidence between the evaluative and control aspects, and it represents the beliefs of the investor before his or her intention to invest: a person with a positive attitude toward investing and a positive sense of being able to invest safely is more likely to intend to invest.

Protection Motivation Theory

Protection motivation theory (Rogers, 1975) predicts the reaction people have to threats. It suggests people estimate both the danger (how serious the danger is and how vulnerable they are to it) and their ability to deal with it (how effective a response would be and how they can be successful at carrying it out). Some users take action to protect themselves while others refuse to use the technologies; this theory has been adapted by security researchers to explain this phenomenon (Ifinedo, 2012; Liang & Xue, 2009). In terms of investing, cybersecurity threat awareness enhances coping appraisal, meaning that an investor who is aware of the threats knows how to respond to them. By contrast, perceived cybersecurity risk involves threat appraisal but without a sense of control. Thus, protection motivation theory predicts that there should be opposite relationships of awareness and perceived risk with confidence and intention.

Trust–Risk Perspective

These theories are complemented by the trust–risk theory of electronic commerce (Kim et al., 2008; Pavlou, 2003), which focuses on the trust and perceived risk of online transactions. Perceived risk has the opposite effect of trust: trust increases the willingness to transact and decreases the perceived risk, and vice versa. Gefen et al. (2003) demonstrated that trust plays the same role as the usefulness of the technology in predicting online behaviour. Trust is the equivalent of investor confidence in a digital stock market, which is connected to investors' perceptions and participation.

CONCEPTUAL FRAMEWORK AND HYPOTHESES

The conceptual framework is shown in Figure 1. The independent variables are cybersecurity threat awareness and cybersecurity perceived risk, the proposed intervening variable is the investor's confidence, and the outcome is the stock market participation intention. The present analysis is correlational; the direction of the arrows in the figure represents the theoretical considerations and are presented here for testing with causal designs in subsequent analyses.

ISSN (Print): 2959- 099X ISSN (Online): 2959-1007
Volume 5, Issue 1, Page 65-84, June 30, 2026

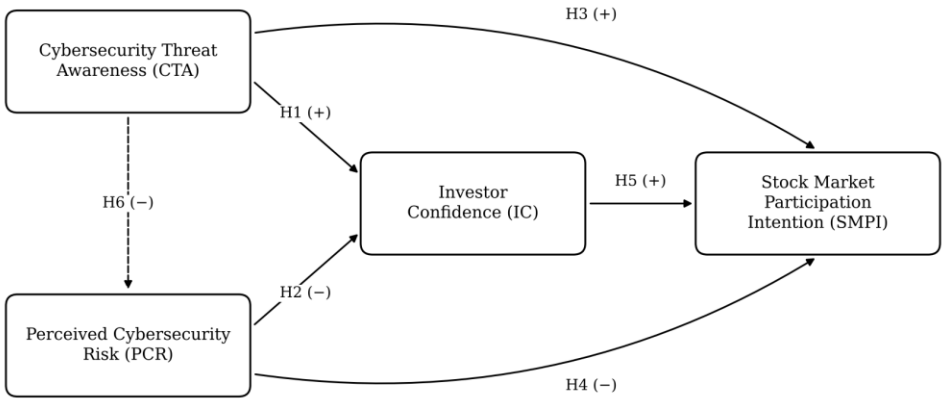


Figure 1: Conceptual framework of the study

Note. Solid arrows represent hypothesized associations between investor confidence and intent to participate; dashed arrows represent hypothesized associations between the two independent variables.

From the literature and theory reviewed above, the following hypotheses are formulated:

H_1: Investor confidence is positively related to cybersecurity threat awareness.

H_2: Investor confidence is negatively correlated with perceived cybersecurity risk.

H_3: Cybersecurity threat awareness is positively related to the intention to participate in the stock market.

H_4: The perceived cybersecurity risk negatively influences the intention to participate in the stock market.

H_5: There is a positive relationship between investor confidence and intention to participate in the stock market.

H_6: Cybersecurity threat awareness is negatively related to the perceived cybersecurity risk.

RESEARCH METHODOLOGY

Research Design

The research was based on the positivist philosophy and deductive approach which tested the hypotheses from existing theory. Data collection utilized a quantitative cross-sectional survey design, suitable for measuring perceptions and examining relationships among variables at one time.

Population and Sample

The population consisted of individual (retail) investors of Pakistan having an active trading account with a brokerage firm registered with the Pakistan Stock Exchange (PSX). As no complete sampling frame of retail investors was available to the researchers, the researchers used the non-probability technique of purposive sampling: respondents were eligible only if they had invested in listed equities at least once. For a large population, Krejcie and Morgan (1970) suggest the need for a minimum sample size of approximately 384 at the 95% confidence level. The final sample of 400 usable responses is above this and also meets common rules of thumb for multivariate analysis (Hair et al., 2019).

Instrument and Measures

A structured questionnaire was used with two parts to collect data. The first part (Part A) collected demographic data (gender, age, education, investment experience). The four study constructs were assessed using 20 items, five items per construct, rated on a 5-point Likert scale from 1 to 5, strongly disagree to strongly agree (SA), respectively. Items were adapted from existing sources and reworded for the stock trading context. Items related to cybersecurity threat awareness were based on the information security awareness items of Bulgurcu et al. (2010). The perceived cybersecurity risk items were adapted from the financial and privacy risk facet of Featherman and Pavlou (2003). The items measuring investor confidence were adapted from the trust measures used by Gefen et al. (2003) and Kim et al. (2008). The items used to measure the intention to participate in the stock market were based on the intention to act items suggested by Ajzen (1991) and adapted to online trading by Lee (2009). The questionnaire was given to subject-matter experts to check the content validity and also pre-tested with a small number of students before its administration.

Ethics and Data Collection

The questionnaire was administered in person and via brokerage networks and investor groups on the Internet. The study was done on a voluntary basis, no personal information was collected and participants were informed of the purpose of the study. Participants were assured that their responses would only be used as aggregates for academic purposes. To minimize common method bias, the questionnaire was divided into independent measures or predictor items and outcome items and the items were worded in a neutral manner with the items in the outcome section being constructed to not share commonalities with the items in the predictor section, consistent with the procedural remedies recommended by Podsakoff et al. (2003).

Data Analysis Techniques

Data were analysed with SPSS software. The respondents' demographic profile was described using frequency analysis, central tendency and dispersion of each construct were summarized using descriptive statistics and Cronbach's alpha was used to test for internal consistency with a minimum acceptable value of .70 (Nunnally & Bernstein, 1994), and the hypothesized associations were tested using Pearson's product-moment correlation. Cohen's (1988) criteria for the strength of correlation

ISSN (Print): 2959- 099X ISSN (Online): 2959-1007
Volume 5, Issue 1, Page 65-84, June 30, 2026

were adopted and correlations of .10, .30 and .50 were interpreted as small, medium and large effects, respectively.

ANALYSIS AND INTERPRETATION

Demographic Profile

Table 1: Demographic Profile of Respondents (N = 400)

Demographic Variable	Categories	Frequency	Percentage (%)
Gender	Male	250	62.5
	Female	150	37.5
Age	18–25 years	100	25.0
	26–35 years	145	36.3
	36–45 years	100	25.0
	Above 45 years	55	13.7
Education	Bachelor's	160	40.0
	Master's	180	45.0
	MPhil/PhD	60	15.0
Investment Experience	< 1 year	110	27.5
	1–3 years	145	36.3
	4–6 years	90	22.5
	Above 6 years	55	13.7
Total		400	100.0

As can be seen in Table 1, 62.5% of the sample was male and 37.5% were female. This imbalance is not unusual in equity markets in Pakistan and in many South Asian countries, where women are under-represented in the active investor population and is consistent with other evidence that suggests men are more likely to be active traders than women in stock markets (Barber & Odean, 2001).

In terms of age, the largest group (36.3%) was between 26 and 35 years old, followed by equal shares (25.0% each) of investors aged 18–25 and 36–45. Only 13.7% were older than 45. Combined, approximately 61% of respondents were 35 or younger. The younger investor profile is significant for the study as they are more likely to be trading through mobile apps and online platforms and are thus more vulnerable to cyber threats.

The sample was well educated, with 45.0% having a master's degree, 40.0% a bachelor's degree and 15.0% having an MPhil or PhD. As a result, each of the respondents had a minimum of an undergraduate education, which ensures that the data on technical issues like phishing and account security is reliable, but may also result in a more educated sample of Pakistani investors than the average investor.

Experience in investing was distributed by investment categories. A third of respondents (36.3%) reported having one to three years of experience and 27.5% less than one year. Thus nearly two-thirds of respondents (63.8%) had three years of experience or less, while 36.2% had more than three years. The proportion of relatively new investors aligns with the recent rise of digital onboarding, which indicates that cyber perceptions can be particularly relevant at the initial stages of an investor's journey.

Descriptive Statistics

Table 2: Descriptive Statistics of Study Variables

Variable	N	Minimum	Maximum	M	SD
Cybersecurity Threat Awareness	400	1.00	5.00	3.82	0.76
Perceived Cybersecurity Risk	400	1.00	5.00	3.67	0.81
Investor Confidence	400	1.00	5.00	3.54	0.79
Stock Market Participation Intention	400	1.00	5.00	3.61	0.83

Note. Each item of the variables used a five-point Likert scale (1 = strongly disagree, 5 = strongly agree).

As indicated in Table 2, the mean scores were in all cases above the scale midpoint of 3.00 and all responses from the 1 to 5 scale were included for all variables. The mean (M = 3.82, SD = 0.76) for cybersecurity threat awareness was the highest. This suggests that, on average, respondents believed that they had a “reasonable knowledge of cyber threats like phishing and account fraud”. The relatively low standard deviation indicates that this attitude was quite common among the respondents.

Perceived cybersecurity risk was also very high (M = 3.67, SD = 0.81). Investors, in other words, knew about cyber threats, but were worried. An interesting finding is that even when investors were aware of the threats, they were not indifferent to them; they were both aware of the threats and perceived them as risky.

The Investor Confidence construct had the lowest mean of the four constructs (M = 3.54, SD = 0.79). This is still above the halfway mark, but indicates a moderate level of confidence in the security and reliability of the market and digital platforms. Generally speaking, the intention to participate in the stock market was moderate (M = 3.61) and the most dispersed (SD = 0.83), indicating that investors varied more in terms of their future plans than in their perceptions. Overall, it is a picture of an informed and willing investor base that has more confidence to build on.

ISSN (Print): 2959- 099X ISSN (Online): 2959-1007
Volume 5, Issue 1, Page 65-84, June 30, 2026

Reliability Analysis

Table 3: Reliability Analysis of Study Constructs

Construct	Number of Items	Cronbach's α
Cybersecurity Threat Awareness	5	0.861
Perceived Cybersecurity Risk	5	0.884
Investor Confidence	5	0.897
Stock Market Participation Intention	5	0.872
Overall Scale	20	0.914

Note. Values of 0.70 or greater were considered to represent acceptable internal consistency (Nunnally & Bernstein, 1994).

As shown in Table 3, all four constructs met the 0.70 level recommended by Nunnally and Bernstein (1994). The Cronbach's alpha coefficient was between .861 and .897, which are considered good (Hair et al., 2019) with values above .80. Within each scale, items thus measured the same construct that they were designed to measure.

The overall 20 item scale gave an alpha coefficient of .914, indicating excellent internal consistency for the instrument. The statements for investor confidence had the highest reliability, indicating that the respondents understood the statements related to investor confidence very uniformly. There were no redundant items as none of the alpha values was greater than .95. With these results, the composite construct scores were used for the correlation analysis that follows.

Correlation Analysis

Table 4: Pearson Correlation Analysis

Variable	1	2	3	4
1. Cybersecurity Threat Awareness	1			
2. Perceived Cybersecurity Risk	−.310**	1		
3. Investor Confidence	.520**	−.460**	1	
4. Stock Market Participation Intention	.490**	−.420**	.610**	1

Note. N = 400. ** $p < .01$ (two-tailed).

Pearson correlation coefficients for the four constructs are given in Table 4. Each coefficient was significant at the .01 level and all of them had the predicted sign.

Investor confidence was significantly ($r = .520$, $p < .01$) and positively related to cybersecurity threat awareness, supporting H1. In Cohen's (1988) classification, this is a large effect, with awareness and confidence sharing 27% of the variance. Investors with a better understanding of cyber threats are more likely to feel confident about the

market, which aligns with the notion of the benefits of a sense of control, which can be strengthened by knowledge.

This finding supported H2, as perceived cybersecurity risk was negatively correlated with investor confidence ($r = -.460$, $p < .01$). This medium effect suggests that investors who feel more threatened by cyber loss are less confident in the security and reliability of the market (21% shared variance).

The results further supported H3, with a positive association between cybersecurity threat awareness and stock market participation intention ($r = .490$, $p < .01$), and H4, with a negative association between perceived cybersecurity risk and stock market participation intention ($r = -.420$, $p < .01$). Both are medium to large effects. The two findings of this study are opposing: Awareness and perceived risk have to do with cyber threats, but they are associated with participation in different ways.

The matrix showed that investor confidence had the highest correlation with intention of participating in the stock market ($r = .610$, $p < .01$) and it supported H5. Confidence accounts for approximately 37% of the variance of intention, making it the most related variable to the participation. Additionally, its correlation with both awareness and perceived risk is greater than that of awareness and risk with intention, reflecting the fact that both awareness and risk may be correlated with intention, but that perceived risk is larger; this possibility should be formally examined using mediation analysis.

Lastly, cybersecurity threat awareness was negatively associated with perceived cybersecurity risk ($r = -.310$, $p < .01$), lending support to H6. In size, the effect is medium with 10% of shared variance accounted for. Well-informed investors feel a little less risk and the small size of the coefficient indicates that "awareness" and "perceived risk" are two separate and distinct concepts. None of the coefficients was close to .80 or greater, indicating that multicollinearity is not a problem (Hair et al., 2019).

ISSN (Print): 2959- 099X ISSN (Online): 2959-1007
Volume 5, Issue 1, Page 65-84, June 30, 2026

Summary of Hypothesis Testing

Table 5: Summary of Hypothesis Testing

Hypothesis	Path	r	Decision
H_1	CTA → IC (+)	.520**	Supported
H_2	PCR → IC (−)	−.460**	Supported
H_3	CTA → SMPI (+)	.490**	Supported
H_4	PCR → SMPI (−)	−.420**	Supported
H_5	IC → SMPI (+)	.610**	Supported
H_6	CTA → PCR (−)	−.310**	Supported

Note. CTA = Cybersecurity threat awareness; PCR = Perceived cybersecurity risk; IC = Investor confidence; SMPI = Stock market participation intention. ** $p < .01$.

Table 5 shows that all six hypotheses were supported. The directions of all associations were as predicted and the effect sizes were moderate to large.

DISCUSSION

The purpose of this study was to gain insight into the relationship between investors' perception of cybersecurity, their confidence, and their willingness to invest in the stock market. The results paint a consistent picture. Investors who are knowledgeable about cyber threats are more confident and more likely to invest, and investors who feel exposed to cyber risk are less confident and less likely. Investor confidence is the factor most associated with participation intention.

The positive relationships between threat awareness and confidence (H1) and threat awareness and intention (H3) should be highlighted as these contradict a widely held concern that discussing cyber threats will deter investors. The results indicate otherwise. This mirrors protection motivation theory (Rogers, 1975) in that threats that are coupled with coping ability elicit a constructive response to threat. It is also in line with Boss et al. (2015) indicating that efficacy messages are more successful in communicating fear appeals, and Bulgurcu et al. (2010) revealing that awareness is a precursor to positive beliefs regarding protective behaviors. An informed investor understands the significance of using two-factor authentication, spotting a scam, and picking a secure broker; it seems investment knowledge becomes investment confidence.

The negative relationship between perceived cybersecurity risk and confidence and intention (H2 and H4) is similar to the perceived-risk literature (Featherman & Pavlou, 2003; Pavlou, 2003) and to the Kim et al. (2008) trust–risk model, in which perceived risk undermines trust and reduces the desire to transact. It is also consistent with Slovic's (1987) statement that risks that are unfamiliar and

uncontrollable elicit potent responses. From an investor-level perspective, the finding provides an explanation for the market price reactions in breach event studies that have been observed (Ali et al., 2021; Cavusoglu et al., 2004; Kamiya et al., 2021): as cyber incidents increase the perceived threat, investor-level confidence should be expected to decline, thereby reducing investor demand for shares.

H5 is supported by the strong relationship between investor confidence and participation intention, which is consistent with the existing body of research on the relationship between investor confidence and participation in household finance. Guiso et al. (2008) and Georgarakos and Pasini (2011) demonstrated the positive relationship between trust and stock ownership. Adil et al. (2023) revealed that trust in financial institutions had the highest relationship with participation intention among the investors in India. The present study builds on this previous work by demonstrating that trust in a digital market is also related to cyber perceptions. According to the theory of planned behavior (TPB) (Ajzen, 1991), confidence reflects much of the positive attitude and perceived control that result in intention.

A modest negative correlation is observed with respect to the awareness–perceived risk relationship (H6). This is only a partial reduction of perceived risk, and the descriptive results indicate that investors reported this risk to be high, as well as the other risk factor. It indicates that people who know a lot are not complacent; they still believe there is real risk, but they believe they can control it. Policy messages should not be geared to convincing investors that there is little cyber risk, but to helping them to understand and manage it.

The pattern of correlations suggests that a model of the form of awareness and perceived risk influences confidence which in turn influences intention is plausible. Investor confidence had the lowest mean score of any of the four constructs, and is thus seen to be the core area for improvement. Since confidence is based on cyber perceptions and participation, activities which increase confidence will likely have the most impact on market participation.

CONCLUSION

Cybersecurity is now a part of the routine calculations made by investors when they consider whether or not to join or remain in the stock market. This study revealed that investor confidence and intention to invest are positively related to cybersecurity threat awareness, while perceived cybersecurity risk is negatively related to both these constructs, using the survey data from 400 retail investors of Pakistan. The relationship between investor confidence and participation intention was the strongest, with perceived risk having a modest relationship. All six hypotheses were supported, and the scales used for measuring were found to be quite reliable.

The principal takeaway is that knowledge and fear are different. Knowing about cyber threats makes investors more eager to get involved, while a lack of understanding of the risks reduces confidence. If market expansion is the goal, the focus should be on converting fear into educated confidence, by educating the investor and visibly securing the platform he or she uses.

ISSN (Print): 2959- 099X ISSN (Online): 2959-1007
Volume 5, Issue 1, Page 65-84, June 30, 2026

RECOMMENDATIONS

Based on the results, the following recommendations are made:

- Investor cyber-awareness programs. Security awareness campaigns through the Securities and Exchange Commission of Pakistan, the Pakistan Stock Exchange, and the Central Depository Company should be conducted on a regular basis and should be practical in nature and cover the areas of phishing, security of accounts and reporting of frauds. As awareness was associated with increased confidence, this education will likely encourage people to participate rather than dissuading them.

- Adopting a policy of "visible security assurance" by brokers. The communication of the security measures by the brokerage firms, such as two-factor authentication, login alerts, trade alerts, and encryption, should be clearly communicated to investors, to show them that their account is secure. When security is visible, it can reduce the perceived risk and increase confidence.

- Baseline security requirements. Regulators need to specify and enforce minimal cybersecurity requirements on trading platforms, including frequent audits and penetration testing, to lower investors' risk perception.

- Clear incident disclosure and compensation. Proper, timely disclosure and fair investor compensation in the event of a failure in a platform would help put investors at ease that they would not be on the losing side if something goes wrong in the platform that is not their fault.

- Targeting new investors. Twenty percent or more of respondents are new to the industry, with almost two-thirds having three years or less of experience, meaning that onboarding programs should have a brief cybersecurity component from the outset to foster safe practices with new investors.

- Inclusive outreach. Public awareness activities should be targeted towards women and older investors, who were not well represented in the sample, to enable wider and more inclusive participation.

LIMITATIONS AND FUTURE RESEARCH

There are a number of caveats that should be noted. The first is that the cross-sectional, correlational design demonstrates an association but not causation. The conceptual framework has a theoretical underpinning for the direction of the paths but has not been tested in a causal fashion. Further research could be conducted with regression or structural equation modeling, as well as longitudinal designs, and would involve formal testing to determine the mediating role of investor confidence between awareness and intention.

Second, with purposive sampling, the results will not be generalizable. The sample was youthful, educated and mostly male and not necessarily a representative sample of all the Pakistani investors. Third, self-report was used to collect all data from a single source, which increases the likelihood of social desirability and common

method bias despite the methods of data collection employed (Podsakoff et al., 2003). Fourth, the study was based on survey responses rather than actual trading actions, which would enhance future research.

Lastly, other important factors that might influence the decision to invest were not included in the model, including financial literacy, risk tolerance, prior experience of cyber fraud, and demographic factors. These variables can be added in future studies, and investors can be studied from country to country, along with an analysis of the impact of certain security features on investors' perceptions over time.

SIGNIFICANCE OF THE STUDY

- **Theoretical significance.** The study integrates theory of planned behavior, protection motivation theory, and the trust–risk perspective to account for investment attitude in a digital environment. It indicates that cyber threat awareness and cyber risk perception are two contrasting constructs, with opposing relationships, and it places investor confidence as the bridge to participation. It brings cyber-risk research in finance from firm-level price reactions to investor-level perceptions.

- **Practical significance.** Regulators and exchanges will look at the findings and see that cyber-awareness education can help rather than hinder the development of the markets. They provide brokerage firms with a glimpse into the reality that security is not just a technical matter but a cornerstone of trust and, ultimately, business development. The study highlights the importance of the role of cyber risks in responsible investing for investors.

- **Contextual significance.** The study offers limited insights into the retail adoption rate in Pakistan and South Asia, which is relatively low, and digital onboarding is growing. The findings can be used as a blueprint for policy in other emerging markets with similar issues as they attract investors to digital platforms.

AUTHOR NOTE

Correspondence concerning this article should be addressed to Mubasir Qadir. The authors declare no conflict of interest. No external funding was received for this study.

REFERENCES

Adil, M., Singh, Y., & Ansari, M. S. (2023). Do trust in financial institution and financial literacy enhances intention to participate in stock market among Indian investors during COVID-19 pandemic? *Cogent Economics & Finance, 11*(1), Article 2169998. https://doi.org/10.1080/23322039.2023.2169998

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

ISSN (Print): 2959- 099X ISSN (Online): 2959-1007
Volume 5, Issue 1, Page 65-84, June 30, 2026

Ali, S. E. A., Lai, F.-W., Dominic, P. D. D., Brown, N. J., Lowry, P. B., & Ali, R. F. (2021). The long-run impact of information security breach announcements on investors' confidence: The context of efficient market hypothesis. *Sustainability, 13*(3), Article 1066. https://doi.org/10.3390/su13031066

Balloch, A., Nicolae, A., & Philip, D. (2015). Stock market literacy, trust, and participation. *Review of Finance, 19*(5), 1925–1963. https://doi.org/10.1093/rof/rfu040

Barber, B. M., & Odean, T. (2001). Boys will be boys: Gender, overconfidence, and common stock investment. *The Quarterly Journal of Economics, 116*(1), 261–292. https://doi.org/10.1162/003355301556400

Bauer, R. A. (1960). Consumer behavior as risk taking. In R. S. Hancock (Ed.), *Dynamic marketing for a changing world* (pp. 389–398). American Marketing Association.

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS Quarterly, 39*(4), 837–864. https://doi.org/10.25300/MISQ/2015/39.4.5

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly, 34*(3), 523–548. https://doi.org/10.2307/25750690

Campbell, K., Gordon, L. A., Loeb, M. P., & Zhou, L. (2003). The economic cost of publicly announced information security breaches: Empirical evidence from the stock market. *Journal of Computer Security, 11*(3), 431–448. https://doi.org/10.3233/JCS-2003-11308

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). The effect of Internet security breach announcements on market value: Capital market reactions for breached firms and Internet security developers. *International Journal of Electronic Commerce, 9*(1), 70–104. https://doi.org/10.1080/10864415.2004.11044320

Cohen, J. (1988). *Statistical power analysis for the behavioral sciences* (2nd ed.). Lawrence Erlbaum Associates.

Ebrahimi, S., & Eshghi, K. (2022). A meta-analysis of the factors influencing the impact of security breach announcements on stock returns of firms. *Electronic Markets, 32*(4). https://doi.org/10.1007/s12525-022-00550-2

Featherman, M. S., & Pavlou, P. A. (2003). Predicting e-services adoption: A perceived risk facets perspective. *International Journal of Human-Computer Studies, 59*(4), 451–474. https://doi.org/10.1016/S1071-5819(03)00111-3

Florackis, C., Louca, C., Michaely, R., & Weber, M. (2023). Cybersecurity risk. *The Review of Financial Studies, 36*(1), 351–407. https://doi.org/10.1093/rfs/hhac024

Förderer, J., & Schuetz, S. W. (2022). Data breach announcements and stock market reactions: A matter of timing? *Management Science, 68*(10), 7298–7322.

Gefen, D., Karahanna, E., & Straub, D. W. (2003). Trust and TAM in online shopping: An integrated model. *MIS Quarterly, 27*(1), 51–90. https://doi.org/10.2307/30036519

Georgarakos, D., & Pasini, G. (2011). Trust, sociability, and stock market participation. *Review of Finance, 15*(4), 693–725. https://doi.org/10.1093/rof/rfr028

Guiso, L., Sapienza, P., & Zingales, L. (2008). Trusting the stock market. *The Journal of Finance, 63*(6), 2557–2600. https://doi.org/10.1111/j.1540-6261.2008.01408.x

Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2019). *Multivariate data analysis* (8th ed.). Cengage Learning.

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security, 31*(1), 83–95. https://doi.org/10.1016/j.cose.2011.10.007

International Monetary Fund. (2024). *Global financial stability report: The last mile: Financial vulnerabilities and risks* (Chapter 3: Cyber risk: A growing concern for macrofinancial stability). International Monetary Fund.

Kahneman, D., & Tversky, A. (1979). Prospect theory: An analysis of decision under risk. *Econometrica, 47*(2), 263–291. https://doi.org/10.2307/1914185

Kamiya, S., Kang, J.-K., Kim, J., Milidonis, A., & Stulz, R. M. (2021). Risk management, firm reputation, and the impact of successful cyberattacks on target firms. *Journal of Financial Economics, 139*(3), 719–749. https://doi.org/10.1016/j.jfineco.2019.05.019

Kannan, K., Rees, J., & Sridhar, S. (2007). Market reactions to information security breach announcements: An empirical analysis. *International Journal of*

ISSN (Print): 2959- 099X ISSN (Online): 2959-1007
Volume 5, Issue 1, Page 65-84, June 30, 2026

Electronic Commerce, 12(1), 69–91. https://doi.org/10.2753/JEC1086-4415120103

Kim, D. J., Ferrin, D. L., & Rao, H. R. (2008). A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents. *Decision Support Systems, 44*(2), 544–564. https://doi.org/10.1016/j.dss.2007.07.001

Krejcie, R. V., & Morgan, D. W. (1970). Determining sample size for research activities. *Educational and Psychological Measurement, 30*(3), 607–610. https://doi.org/10.1177/001316447003000308

Lee, M.-C. (2009). Predicting and explaining the adoption of online trading: An empirical study in Taiwan. *Decision Support Systems, 47*(2), 133–142. https://doi.org/10.1016/j.dss.2009.02.003

Liang, H., & Xue, Y. (2009). Avoidance of information technology threats: A theoretical perspective. *MIS Quarterly, 33*(1), 71–90. https://doi.org/10.2307/20650279

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *Academy of Management Review, 20*(3), 709–734. https://doi.org/10.5465/amr.1995.9508080335

Nunnally, J. C., & Bernstein, I. H. (1994). *Psychometric theory* (3rd ed.). McGraw-Hill.

Pavlou, P. A. (2003). Consumer acceptance of electronic commerce: Integrating trust and risk with the technology acceptance model. *International Journal of Electronic Commerce, 7*(3), 101–134. https://doi.org/10.1080/10864415.2003.11044275

Podsakoff, P. M., MacKenzie, S. B., Lee, J.-Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: A critical review of the literature and recommended remedies. *Journal of Applied Psychology, 88*(5), 879–903. https://doi.org/10.1037/0021-9010.88.5.879

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology, 91*(1), 93–114. https://doi.org/10.1080/00223980.1975.9915803

Rosati, P., Cummins, M., Deeney, P., Gogolin, F., van der Werff, L., & Lynn, T. (2017). The effect of data breach announcements beyond the stock price: Empirical evidence on market activity. *International Review of Financial Analysis, 49*, 146–154. https://doi.org/10.1016/j.irfa.2017.01.001

Slovic, P. (1987). Perception of risk. *Science, 236*(4799), 280–285. https://doi.org/10.1126/science.3563507

van Rooij, M., Lusardi, A., & Alessie, R. (2011). Financial literacy and stock market participation. *Journal of Financial Economics, 101*(2), 449–472. https://doi.org/10.1016/j.jfineco.2011.03.006