Human Behavior, Development and Society
E-ISSN 2651-1762, Vol 24 No 3, December 2023

Roles of Perceived Knowledge, Risk, and Trust in Cybersecurity Solution Implementation: A Study in Bangkok, Thailand

T Dau Naw and Phanasan Kohsuwan, Panyapiwat Institute of Management, Thailand

Date Received: 24 August 2023 Revised: 1 October 2023 Accepted: 3 October 2023

Abstract

Thailand has adopted an economic model (Industrial 4.0) that merges physical manufacturing processes and services with digital connectiveness. Hence, cybersecurity cannot be ignored. The aim of this research was to promote cybersecurity awareness among technology and information executives, along with top-level managers, develop a more efficient security management system, and implement an effective cybersecurity framework for the private and public sectors in Thailand. An extension of the Technology Acceptance Model was developed that used three variables, namely, perceived knowledge of cybersecurity, perceived risk of cyberattacks, and perceived trust in cybersecurity solutions. A quantitative research approach was used to collect data from both online and offline survey forms (*N* = 394). Exploratory Factor Analysis, Confirmatory Factor Analysis, and Structural Equation Modeling were used to analyze this data. The findings permitted the Technology Acceptance Model to be extended. Positive relationships were found among perceived knowledge of cybersecurity, perceived risk of cyberattacks, and perceived trust in cybersecurity solutions. These variables, together with perceived ease of use, usefulness, and attitude towards using cybersecurity solutions, all played a pivotal role in organizations/businesses in Thailand and their intention to implement cybersecurity solutions.

Keywords: *Technology acceptance, cybersecurity, perceived knowledge, risk, trust*

Introduction

Decades ago, before computers had become a part of our lives and the Internet also played an essential role in our daily lifestyles, the term “cybersecurity” was not something we were aware of like today. Thanks to industrial revolutions and the Internet of Things, the value of human treasures has shifted from natural resources, such as gas and oil, to the precious gems of data and intellectual property (The Economist, 2017). Morgan (2020) pointed out that data protection is the phenomenon of our time, the world’s new natural resource. A cyberattack could potentially disable the economy of a city, a state, or even an entire country. A data breach can have far-reaching consequences, causing financial losses and affecting an organization’s operations and compliance in the short term. Furthermore, a major breach in the headlines can potentially damage reputations for years to come, leading to lost business and a competitive disadvantage.

Security threats are constantly evolving as cyber criminals become more sophisticated at targeting valuable commercial and organizational resources. Cyber threats are a ubiquitous problem for every business, with many companies struggling to improve their cyber awareness. The post COVID-19 pandemic is still being leveraged by cybercriminals for illicit profit. Management of any organization must understand that the cost of a cyber breach is very expensive and in the criminal mind, targetting is based on the size of the organization. Therefore, allocating some budget for cybersecurity may not directly increase the company’s return on investment, but the expenditure is justified if setting aside those funds may save the company from unexpected potential losses arising from a cyberattack.

According to the National Cyber Security Agency (NCSA) (2023), the number of cybersecurity threats in Thailand rose significantly from 135 incidents in 2021 to over 772 incidents in 2022. Website hacking was two to three times more common than other forms of cyberattacks in Thailand. Educational and public health agencies’ websites were the most frequent targets of cyberattacks, especially those sites accessed by many people. Cybercrimes could cost Thailand’s

economy an estimated 286 billion Baht, i.e., 2.2% of the total country's GDP, and the dramatic rise in damage costs means there are still many businesses and organizations in Thailand that are not yet prepared against cyberattacks (Fung, 2023). Recently, Thailand implemented the Cybersecurity Act of B.E. 2562 (2019) to maintain national cybersecurity in order to enhance the immunity of both the private and public sectors. These initiatives have promoted collaboration among domestic and international organizations and increased vigilance against cyber threats through developing cybersecurity personnel, raising awareness among the public, and upgrading critical information infrastructure and government agencies (NCSA, 2023). Based on observation of current technological disruptions in Thailand's digital private and public sectors, the following questions were raised to address the needs for tackling the cyberattacks Thailand has been facing.

1. Why is it that both the private and public sectors in Thailand do not take cybersecurity as seriously as they should?
2. How essential is cybersecurity knowledge and/or awareness for chief technology, information, and executive officers, along with managers in organizations/ businesses, especially during this post-COVID 19 pandemic recovery time?
3. What are the influential factors that both the private and public sectors should be aware of when implementing cybersecurity infrastructure in their organizations/businesses?

The aim of the research was initially to promote cybersecurity awareness, develop a more efficient security management system in each business/organization, and then implement an overall better cybersecurity framework for both the private and public sectors in Thailand. The primary research objectives were to provide an extensive literature review, to detail business practices, particularly in Thailand, regarding shortfalls in current operations, and to map out a conceptual framework to provide for more secure and trusted business operations nationwide so as to align with global security policies. In addition, the study covered in-depth insights on the following sub-objectives:

1. To explore the factors that businesses take into consideration when planning to implement cybersecurity solutions.
2. To investigate how perceived knowledge, perceived risk, perceived trust, perceived ease of use, perceived usefulness, and attitude affect the behavioral intention to use cybersecurity solutions.
3. To propose an extension of the Technology Acceptance Model (TAM) with expanded variables to help build cybersecurity awareness of chief technology, information, and executive officers, along with managers in Thailand's private and public sectors to help them engage more seriously with adopting cybersecurity solutions.

Literature Review

Both the private and public sectors of a country, including its government agencies, need to take a comprehensive approach to cybersecurity rather than an ad hoc approach of dealing with threats on a case-by-case basis as they are discovered. Security should be viewed in the context of processes, and not specific technological fixes (Bhuyan, et al., 2020). Davis et al. (1989) developed a theory called the Technology Acceptance Model that demonstrates how individuals make a decision to accept and utilize a particular technology. The TAM focuses on the contributions of perceived ease of use and usefulness, along with attitude toward the behavior, in predicting and explaining behavioral intention to actually use the technology. Hansen et al. (2017) elaborated more on TAM and the Theory of Planned Behavior. A series of technology acceptance models have been developed, and among them, the TAM has been most commonly adopted by various researchers (Minghao & Wei, 2021). Perceived ease of use and usefulness, and attitude towards use were originally incorporated as factors in TAM that influenced the acceptance of technology. Continual modifications have been made to this model (Al-Zahrani, 2020). Thus, it was adopted and applied in the present research for investigating cybersecurity awareness and implementation of cybersecurity solutions.

The original definitions of each variable taken from previous studies and the operational definitions applied in this study are presented in Table 1.

Table 1 *Definitions of Terms*

Variables	Definitions	Operational Definitions
Perceived Knowledge	One's self-assessment or feeling of knowing the information needed to evaluate brands in a product class (Park et al., 1987).	A respondent's self-assessment or feeling of knowing the information needed to evaluate proposed cybersecurity solutions.
Perceived Risk	A belief in system characteristics, specifically belief in the competence, dependability, and security of the system, under conditions of risk (Kini & Choobineh, 1998).	A belief in the features of the proposed cybersecurity solutions, specifically a belief in the competence, dependability, and security of the solutions, under conditions of risk.
Perceived Trust	A situation or event where something of human value (including humans themselves) has been put at risk and where the outcome is uncertain (Al-Zahrani, 2020).	A cyberattack or data breach where the hospital (including staff and patients) has been put at risk and where the outcome is uncertain.
Perceived Ease of Use	The degree to which the prospective user expects the target system to be free of effort (Davis et al., 1989).	The degree to which the prospective hospital expects the targeted cybersecurity solution to be free of effort.
Perceived Usefulness	The prospective user's subjective assessment of the probability that using a specific application system will increase his or her job performance within an organizational context (Davis et al., 1989).	The subjective probability held by a prospective business that using a specific cybersecurity solution will increase its performance within an organizational context.
Attitude toward using	An individual's positive or negative perception (evaluative affect) about carrying out the targeted behavior (Ajzen & Fishbein, 1975).	A respondent's positive or negative feelings (evaluative affect) about performing the targeted behavior.
Behavioral Intention to use	A measure of the strength of one's intention to perform a specific behavior (Ajzen & Fishbein, 1975).	A measure of the strength of a respondent's intention to perform a specific behavior.

It is somewhat essential that organizations recognize emerging risks and apply information about cyberthreats coming from both internal and external sources to obtain a better understanding of the tendencies and possible consequence of cybersecurity events (National Institute of Standards and Technology (NIST), 2018). Reaching a critical state of cybersecurity awareness has been one of the most difficult tasks for companies and organizations to achieve in recent times (Bada & Nurse, 2019). People want high-quality information that can help them make an accurate evaluation of risks. Those with a high level of knowledge know the information they need, how to obtain it effectively, and how to comprehend it with less cognitive cost (Zhu et al., 2016). Due to the rising number of cyber incidents and a devastating shortage of technical skills, evaluating the knowledge gap between cybersecurity empowerment and industrial needs is obligatory (Catal et al., 2022).

Similar to financial and reputational risks, cybersecurity risks such as cyberattacks and cybercrimes can affect a company's bottom line by driving up costs, affecting revenue, and damaging an organization's capabilities to gain and retain customers. With an understanding of risk tolerance, organizations can prioritize cybersecurity activities, enabling them to make informed decisions about cybersecurity expenditures (NIST, 2018). Al-Zahrani's (2020) study supported the idea that perceived security and perceived privacy positively impacted perceived risk. Risk perception is a core variable in the Protection Action Decision Model that predicts an individuals'

behavioral responses to risk. Different researchers have measured it using a variety of scales (Zhu et al., 2016).

Researchers frequently quote trust as one of the furthermost perceptions examined in marketing research relationships. Trust has been identified as a major enabler for effective application along with technical innovation adoption (Al-Zahrani, 2020). Coulter and Coulter (2003) claimed that trust was an important factor in the establishment of long-term relationships between business suppliers and their customers, and enhancing trust was especially crucial in service sectors due to the abstract nature of most products or technologies. Bada and Nurse (2019) stated that building a relationship of trust can provide a good basis for engaging with businesses initially and for promoting a cybersecurity culture. Communication becomes a crucial component of engaging with businesses at all points.

In the discourse on privacy implications, organizations may envisage how their cybersecurity solutions might incorporate privacy rules, such as data minimization in the compilation, disclosure, and withholding of personal data related to cybersecurity incidents. In addition, this may involve utilizing inhibitions outside of cybersecurity activities on any data acquired mainly for cybersecurity activities; clarity for specific cybersecurity activities; individual compliance and amendment for contrary impacts emerging from the use of personal data in cybersecurity activities; information quality, accountability, and security; and integrity and scrutiny (NIST, 2018).

Davis et al. (1989) concluded that perceived usefulness is a major determinant of people's intentions to use computers. Their study also indicated that although ease of use is clearly important, the usefulness of a system is even more important and should not be overlooked. Users may be willing to tolerate a difficult interface to access functionality that is very important, while no amount of ease of use will be able to compensate for a system that does not enable a useful task to be completed.

Attitudes toward using a particular system is a major determinant in the intention to use that system. The more positive the attitude, the stronger the behavioral intention, and ultimately the higher is the probability that a corresponding behavior will take place(Ajzen & Fishbein, 1975). The development of cybersecurity performance metrics has been evolving, and businesses should be thoughtful, creative, and careful about the ways in which they employ measurements to optimize use. Thus, organizations need to pinpoint their missions, objectives, and priorities (NIST, 2018).

It is well recognized that an individual's knowledge, skills, and understanding of cybersecurity, as well as their experiences, perceptions, attitudes, and beliefs, are the main influencers of behavior (Bada & Nurse, 2019). Since the 1980s, studies on behavior or behavioral intentions of individuals have been popular in the field of information technology (Minghao & Wei, 2021). An individual's pre-existing beliefs, based on their perceived knowledge, motivates the assessment of information insufficiency. In addition, information seeking triggers risk perception and further influences information processing, and finally stimulates behavioral intentions (Zhu et al., 2015). Kijsanayotin et al. (2009) also found that the perception of possessing knowledge was an aspect of perception of "self-behavior control." Davis et al. (1989) indicated that behavioral intention to use was a major determinant of user behavior, while other variables had an indirect affect through behavioral intention. Three extended variables, namely, perceived knowledge of cybersecurity, perceived risk of cyberattacks, and perceived trust in cybersecurity solutions were used to examine whether the proposed conceptual framework as shown in Figure 1 complied with the research objectives.

Based on the above fine points and rationales, the following hypotheses were formulated:

H_1: Perceived knowledge of cybersecurity positively influences perceived trust in cybersecurity solutions.

H_2: Perceived knowledge of cybersecurity positively influences perceived risk of cyberattacks.

H_3: Perceived trust in cybersecurity solutions positively influences attitudes toward cybersecurity solutions.

H_4: Perceived trust in cybersecurity solutions positively influences perceived ease of use of cybersecurity solutions.

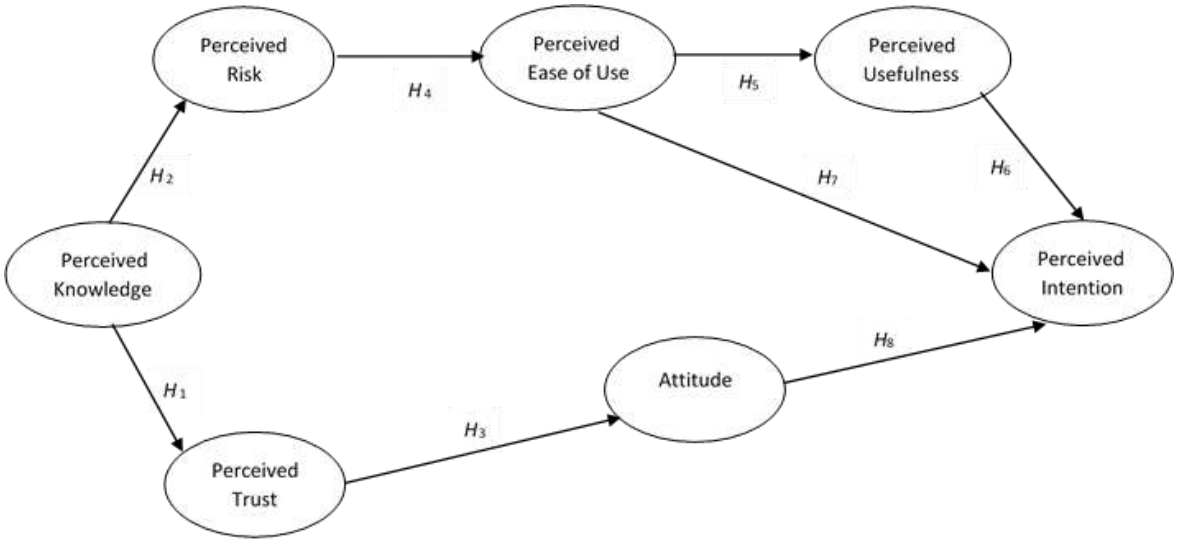
H_5: Perceived ease of use of cybersecurity solutions positively influences perceived usefulness of cybersecurity solutions.

H_6: Perceived usefulness of cybersecurity solutions positively influences behavioral intention to use cybersecurity solutions.

H_7: Perceived ease of use of cybersecurity solutions positively influences behavioral intention to use cybersecurity solutions.

H_8: Attitude toward cybersecurity solutions positively influences behavioral intention to use cybersecurity solutions.

Figure 1 *Conceptual Framework*



Methodology

A quantitative approach was used in the research, as it is observational and uses a theory or hypotheses to bring objectivity. A cross-sectional survey was carried out using a self-administered questionnaire to test the research variables. The respondents were the chief technology, information, and executive officers of firms, individuals from the IT department, or management level employees of companies/organizations from various industries in Thailand. Thirty-one responses were received from an online survey conducted across Thailand for the pilot test. Based on the outcome of the initial analysis, the questionnaires were modified, and some scale items were added for the main study. In the main study, a total of 448 respondents (out of a targeted sample size of 500) participated in the survey. Data was collected both online and using a printed form, but most participants came from the Bangkok Metropolitan area. The response rate was 89.6%. After eliminating incomplete responses and responses with outliers, 394 responses were used in analyzing the roles of the proposed variables.

Frequency analysis was used to summarize the characteristics of respondents in the study. As the targeted sampling group of this research was focused in Thailand, eight demographic attributes were developed, namely, Collection Methods, Gender, Age, Occupation, Industry, Business Type, Working Experience, and Region. The main data were analyzed by applying Structural Equation Modeling to determine if the proposed hypotheses were supported or not. During the process, Confirmatory Factor Analysis was used to validate the model and make it reliable. Exploratory Factor Analysis was employed while running the pilot test as it prepared the variables for a tidier Structural Equation Modeling. In Exploratory Factor Analysis, the Maximum Likelihood Method was used for factor extraction together with the Kaiser-Meyer-Olkin measure and Bartlett's Test for data adequacy. In Confirmatory Factor Analysis, Composite Reliability, Average Variance Extracted, Maximum Shared Variance and Average Shared Variance were calculated to establish adequate validity and reliability.

A structural model was built from the measurement model in SPSS AMOS with statistical support for all the hypotheses gained through global and local tests. Reflective measurement was applied for this quantitative social research as each measure required a proper scale. Likert scaling was utilized for social science information related to attitudes and behavior intentions. The scaled items of all the constructs in the research questionnaire used a five-point Likert scale (1 = *Strongly Disagree*; 2 = *Disagree*; 3 = *Neither Disagree nor Agree*; 4 = *Agree*; 5 = *Strongly Agree*) for data collection.

Findings and Results

The values of the means for all scaled items of the seven variables lay between 3.34 and 4.07. This was above the neutral point of 3.00; thus the respondents as a group held a positive conception of each variable. The closeness of fit of the observations to the structural model, together with the validity and reliability analyses, indicated that all the calculated values met or exceeded the thresholds nominated in Table 3. Thus, the model fitted well. While executing the Confirmatory Factor Analysis in SPSS AMOS, some scaled items were dropped, and some were relocated to other factors according to the suggestions from the modification indices. The Composite Reliability values must be above .70 for good reliability and Average Variance Extracted values must exceed .50 for adequate convergent validity (Hair et al., 2020). The outcome values of the structural model were calculated after running tests and demonstrated distinctive results. Cohen (1988) proposed that if the value of *R*-square for endogenous latent variables is above .75, it indicates a substantial effect; if the value is more than .50, it is taken as moderate, and when the value is less than .25, it is considered weak. Based on author's calculation, the *R*-square value for Perceived Risk was .99, .66 for Perceived Trust, .69 for Perceived Ease of Use, .93 for Perceived Usefulness, .59 for Attitude and .64 for Behavioral Intention. These values are displayed in Figure 2. Hypothesis testing results are shown in Table 4, and indicate that six hypotheses were supported.

Figure 2 *Structural Model Developed from the Authors' Calculations in SPSS AMOS (v. 24)*

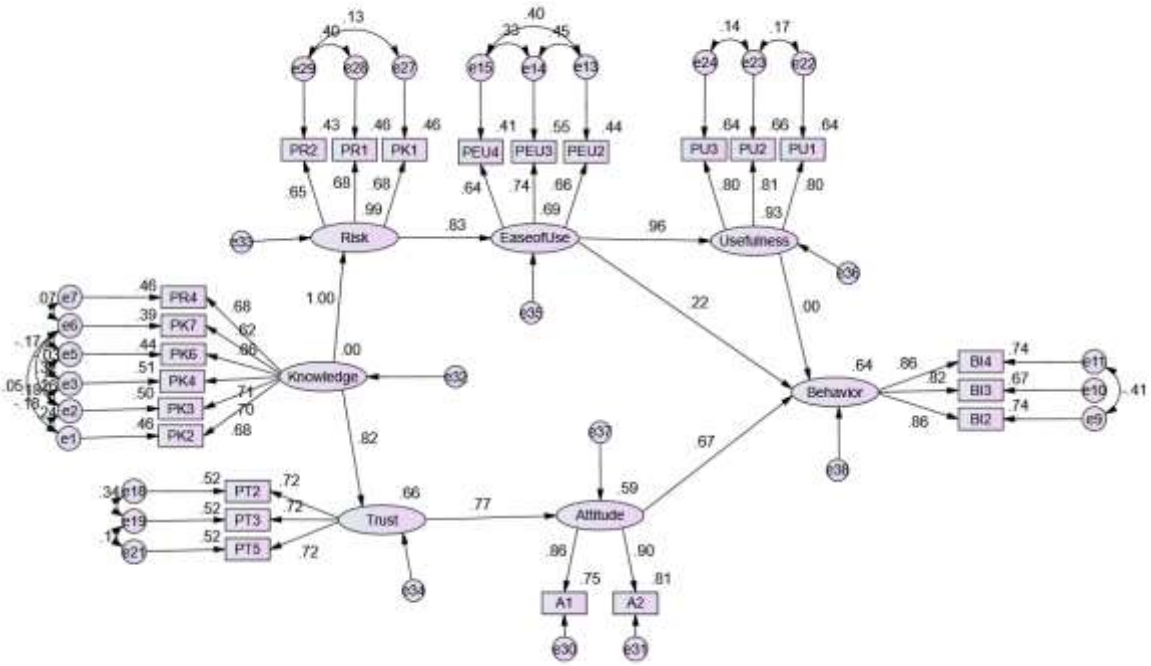


Table 3 *Model Fit Indexes Used for the Structural Model*

Principles	Threshold	Model
Chi-square/*df* (CMIN/*df*)	< 3.00	2.15
p-value	< .05	.00
CFI	> .95	.95
AGFI	> .80	.88
RMSEA	< .05	.05
PCLOSE	> .05	.15

Table 4 *Hypotheses Supported in the Structural Model*

Hypothesis	Path	β	*SE*	CR	*p*-value	Result
H_1	Perceived Knowledge → Perceived Trust	0.815	0.48	15.80	***	Supported
H_2	Perceived Knowledge → Perceived Risk	0.996	0.47	19.32	***	Supported
H_3	Perceived Trust → Attitude	0.768	0.66	14.44	***	Supported
H_4	Perceived Risk → Perceived Ease of Use	0.829	0.07	13.30	***	Supported
H_5	Perceived Ease of Use → Perceived Usefulness	0.963	0.07	15.77	***	Supported
H_6	Perceived Usefulness → Behavioral Intention	-.002	0.44	-0.01	.99	Not supported
H_7	Perceived Ease of Use → Behavioral Intention	0.219	0.50	0.53	.60	Not supported
H_8	Attitude → Behavioral Intention	0.666	0.05	13.16	***	Supported

Code. β = Beta; *SE* = Standard Error; CR = Composite Reliability; *** = *p*-value < .001

Discussion

Based on the research questions, it is evident that government intervention and cooperation among business sectors are pivotal to success in tackling cyberattacks. According to NCSA (2023), Thailand is trying to focus on development of cybersecurity personnel and public awareness by knowledge sharing on cybersecurity, providing academic services on cybersecurity, supporting and arranging for attendance at meetings in accordance with external agencies through the Cybersecurity Policy and Action Plan 2022–2027 in order to ensure economic and social sustainability. The conclusions reached from this study assisted in answering research question 1, and served to illustrate the necessity of cybersecurity awareness among chief technology, information, and executive officers and managers in organizations/businesses. The data also validated the influential factors that all private and public sectors should be aware of before they introduce cybersecurity infrastructural changes in their organizations.

Perceived knowledge of cybersecurity had a positive effect on perceived risk of cyberattacks; this emphasizes the value of both an awareness of the potential benefits of cybersecurity and some knowledge of the impacts of cyberattacks. Trumbo (1999) stated that information processing is another determinant of perceived risk, and Trumbo and McComas (2003) showed that systematic information processing positively influenced perceived risk. Klerck and Sweeney (2007) also agreed that more risk knowledge helps people to achieve a thorough and comprehensive understanding of risk. During the confirmatory factor analysis of our main study, one scaled item from perceived knowledge was loaded under perceived risk and vice versa, which meant that respondents considered perceived knowledge of cybersecurity to interact somewhat with perceived risk of cyberattacks.

Moreover, perceived knowledge of cybersecurity significantly influenced perceived trust in cybersecurity solutions. Faulkner (2011) argued that trust is the parameter that makes it reasonable to depend on the testimony of others. Mortensen and Neeley (2012) also found that both direct and reflected knowledge reinforced trust in explicit ways. Similarly, the research of Zywiolek et al. (2022) showed that trust is influenced by knowledge.

The third hypothesis, involving the influence of perceived trust in cybersecurity solutions on the development of an attitude favouring adoption of cybersecurity solutions, was also supported in this study. The findings of Limbu et al. (2012) indicated that trust enhanced user attitudes toward websites. The relationship between the corporate trustworthiness of an advertiser and attitudes toward the advertisment was mentioned by Sinclair and Irani (2013). They found that trust predicted attitude development. In addition, a positive impact of trust in mobile banking services has been found to impact the development of an attitude of loyalty (Khoa, 2020).

The question of the perceived risk of cyberattacks and perceived ease of use in the adoption of cybersecurity solutions has received some answers from previous researchers. A previous study showed a positive influence of perceived risk on perceived ease of use with a *p*-value less than .05 (Hansen et al., 2017). An interesting outcome of Chen and Aklikokou's (2019) investigation was that technological trust was significantly associated with percevied ease of use, returning a *p*-value of less than .001.

This study demonstrated a positive effect of perceived ease of use of cybersecurity solutions on perceived usefulness of cybersecurity solutions, indicating a strong relationship between the two variables. It is noteworthy that the variables had the highest beta and composite reliability values among all eight hypotheses tested in this research. A previous study by Karim et al. (2020) illustrated the positive relationship between perceived ease of use and perceived usefulness of an e-wallet. Likewise, Sukendro, et al. (2020) claimed that perceived ease of use was the significant predictor of perceived usefulness. Mailizar et al. (2021) agreed that perceived ease of use was a vital aspect in terms of ease of access, capacity of system to meeting users' needs, and flexibililty of the system, and contributed to the perceived usefulness of the e-learning system that they assessed.

One of the two hypotheses not supported in this study was that the perceived usefulness of cybersecurity solutions did not influence behavioral intention to use cybersecurity solutions. Though this result differs from the TAM hypothesis and some previous studies by Humida et al. (2021) and Sukendro, et al. (2020), it is, however, aligned with the findings of Kuo and Yen (2009) and Liao et al.(2007). They found that perceived usefulness had no direct positive effect on behavioral intention to use 3G mobile services.

The other hypothesis that was not supported in this study was that perceived ease of use of cybersecurity solutions did not influence behavioral intention to use cybersecurity solutions. The results showed that perceived ease of use had no significant and positive influence on behavioral intention. In a comparable research study by Kim and Song (2022), perceived ease of use had no significant impact on continuous intention to use Massive Open Online Courses (MOOCs). This was consistent with a study by Alassafi (2022), where the relationship between perceived ease of use and behavioral intention was insignificant. However, TAM has been empirically supported in many research studies, and the hypothesis of perceived ease of use on behavioral intention has been supported by many other researchers (e.g., Karim et al., 2020; Humida et al., 2021; & Basuki, et al., 2021).

The results of tests evaluating the eighth hypothesis affirmed that attitude toward using cybersecurity solutions has a positive and significant influence on behavioral intention to use them. Cao et al. (2021) also confirmed that the behavioral intentions of managers towards using artificial intelligence can be explained and predicted by their attitudes. Similarly, the results of the positive and direct effect of environmental attitude on environmental behavioral intention was statistically significant in a study conducted by Liu et al. (2020). Hwang et al. (2019) also indicated that attitudes toward drone food delivery services positively affected intentions to use the service.

Limitations and Implications

This study was conducted to explore the roles of perceived knowledge, perceived risk, and perceived trust in cybersecurity solutions implementation in Thailand. The analysis of 394 responses collected by both online and offline methods and the statistical findings indicated that the study met its objectives. However, some limitations in this study need to be mentioned. For the demographic

category of “Occupation,” IT Professionals and Other were the most frequently chosen categories. Though a screening question filtered the targeted sample group from random people, the study could not clarify the exact positions that respondents held. Were they involved in the purchasing process of cybersecurity solutions or not? Some industries were not included in this study; this meant that no separation could be established between the private and public sectors in Thailand. In addition, out of 394 participants, 326 respondents were from Bangkok Metropolitan area due to accessibility limitations. The three external factors used were developed based on our observation related to Thailand’s cybersecurity context and all eight hypotheses in this study were exclusively analyzed in a “direct effect” type of hypothesis. The authors chose to conduct an empirical study to examine the roles of perceived knowledge, perceived risk, and perceived trust in cybersecurity solution implementation within the real-world business context.

According to the findings from this study, it can be concluded that since the beginning of post-COVID 19 pandemic recovery time, cybersecurity awareness was obligatory for information and technology executives and managers of organizations and businesses. It is necessary for them to understand the risk of cyberattacks, and this consequently has led them to look for trusted cybersecurity solutions to protect their organizations and businesses. Moreover, despite the fact that Thailand has emphasized the development of competencies in regulatory agencies, government agencies, and critical information infrastructure organizations (NCSA, 2023), our findings indicated that a lack of sufficient knowledge or awareness of cybersecurity, cyberattacks, and attainable solutions for protection. Many private companies and organizations from various industries across Thailand still have not taken cybersecurity as seriously as they should. Businesses need to embrace and adopt automation, big data solutions, and artificial intelligence to cope with the ever-increasing number of alerts and incidents. Therefore, cybersecurity awareness and risk perception of cyberattacks should not be overlooked, especially by people in key positions or holding management level responsibilities. They should keep updated with current cybersecurity trends, as perceived knowledge of cybersecurity has significant impacts on perceived risk of cyberattacks and perceived trust in cybersecurity solutions. Invitations to attend training sessions and conferences aimed to reach organizational or corporate level executives and students might also be extended to government agencies in order to reach a wider audience. This might stimulate greater cybersecurity awareness and exposure if small-to-medium enterprise owners were included, along with those from remote areas. Businesses in Thailand should consider cyber insurance policies and investments in cybersecurity to limit potential damage (Kate, 2021). This is where solution providers who have developed trust and a sound reputation from their current users can play a big part leading new users to adopt useful cybersecurity solutions. This follows from the finding that perceived trust had a positive influence on attitudes toward using cybersecurity solutions, and attitude, in turn, affects behavioral intention.

Providing regular product updates and post-sales services may help in gaining trust from users. Nontheless, both private and public sectors should be aware of not only the fundamental factors such as perceived knowledge on cybersecurity and perceived risk of recent cyberattacks, but also trustworthiness of the solutions, as these factors significantly impact on customer attitudes and behavioral intention to implement cybersecurity infrastructure in their organizations or businesses. Moreover, based on the positive outcomes of the relationships between perceived ease of use and perceived usefulness, cybersecurity solution providers should be aware of the need to emphasize the practicality and convenience of their product in order to promote their use. In the context of this study, perceived ease of use and perceived usefulness of cybersecurity solutions had no significant effect on behavioral intention to use the solutions. This may be due to the fact that consumers are aware of the complexity of the implementation process as per the size of the companies or organizations and that they nevertheless are willing to deploy the solutions regardless based on the cybersecurity criticality of their businesses or organizations. Solutions providers should not overlook the accessibility their product for users, as perceived ease of use on perceived usefulness was strongly supported. Therefore, it is notable that the roles of perceived knowledge of cybersecurity

and perceived risk of cyberattacks, held by those in positions of authority in business/organization, contribute to the implementation of a cybersecurity infrastructure in organizations/businesses in Thailand together with the development of trust in cybersecurity solutions, perceived ease of use, and usefulness of cybersecurity solutions.

Conclusions

The study's main objectives were to promote the awareness or knowledge about cybersecurity, deploy a better security management system with efficiency in businesses and organizations, and implement a more proficient cybersecurity framework in Thailand's private and public sectors. In order to facilitate this, a conceptual model with three extended variables was adopted from the Technology Acceptance Model (TAM), and eight hypotheses were laid out to highlight current business practices in Thailand. Based on the proverb which goes "Prevention is better than cure," this research emphasized three influential factors in addition to those of TAM. Six factors were found to benefit businesses and organizations in Thailand when implementing cybersecurity solutions. These factors were perceived knowledge of cybersecurity, perceived risk of cyberattacks, perceived trust in cybersecurity solutions, perceived ease of use of cybersecurity solutions, perceived usefulness of cybersecurity solutions, and attitude toward using cybersecurity solutions.

Moreover, the results obtained indicated that the three extended factors had a positive influence on behavioral intention to use cybersecurity solutions. Though perceived ease of use and perceived usefulness on behavioral intention were not supported, cybersecurity solution providers should not overlook the importance of the practicality and efficiency of solutions, training, and technical support offered to consumers.

In addition, future researches may consider narrowing the scope of study from the private and public sectors to one specific industry such as finance, healthcare, or tourism. Vague items like "Other" should be avoided as demographic categories, and items need to be carefully prepared to achieve valid responses. Moreover, future scholars may try to obtain a more representative sample of demographic attributes such as gender, age, business type, working experience, and region, to better generalize to the targeted population. For theoretical contribution, future practitioners may include more or different extended variables to TAM, or apply different types of hypotheses such as mediated effects, interaction effects, multi-group effects, mediated moderation, or handling controls by reviewing previous researchers' work. In the future, similar technology studies may adopt the conceptual framework used in this study to examine the roles of perceived knowledge, perceived risk, and perceived trust on other technologies/products and their use.

References

Ajzen, I., & Fishbein, M. (1975). A Bayesian analysis of attribution processes. *Psychological Bulletin, 82*, 261–277. https://doi.org/10.1037/h0076477

Alassafi, M. O. (2022). E-learning intention material using TAM: A case study. *Materialstoday: Proceedings, 61*, 873–877. https://doi: 10.1016/j.matpr.2021.09.457

Al-Zahrani, M. S. (2020). Integrating IS success model with cybersecurity factors for e-government implementation in the Kingdom of Saudi Arabia. *International Journal of Electrical and Computer Engineering (IJECE), 10*(5), 4937–4955. https://doi:10.11591/ijece.v10i5.pp4937-4955

Bada, M., & Nurse, J. R. (2019). Developing cybersecurity education and awareness programmes for small and medium-sized enterprises (SMEs). *Information and Computer Security, 27*(3), 393–410. https://doi: 10.1108/ICS-07-2018-0080

Basuki, R., Tarigan, Z. J., Siagian, H., Limanta, L. S., Setiawan, D., & Mochtar, J. (2021). The effects of perceived ease of use, usefulness, enjoyment and intention to use online platforms on behavioral intention in online movie watching during the pandemic era. *International Journal of Data and Network Science, 6*(1), 253–262. https://doi: 10.5267/j.ijdns.2021.9.003

Bhuyan, S. S., Kabir, U. Y., Escareno, J. M., Ector, K., Palakodeti, S., Wyant, D., Kumar, S., Levy, M., Kedia, S., Dasgupta, D., & Dobalian, A. (2020). Transforming healthcare cybersecurity from reactive to proactive: Current status and future recommendations. *Journal of Medical Systems, 44*(5), 98. https://doi.org/10.1007/s10916-019-1507-y

Cao, G., Duan, Y., Edwards, J. S., & Dwivedi, Y. K. (2021). Understanding managers' attitudes and behavioral intentions towards using artificial intelligence for organizational decision-making. *Technovation, 106,* 102312. https://doi:10.1016/j.technovation.2021.102312

Catal, C., Ozcan, A., Donmez, E., & Kasif, A. (2022). Analysis of cyber security knowledge gaps based on cyber security body of knowledge. *Education and Information Technologies, 28,* 1809–1831. https://doi:10.1007/s10639-022-11261-8

Chen, L., & Aklikokou, A. K. (2019). Determinants of E-government adoption: Testing the mediating effects of perceived usefulness and perceived ease of use. *International Journal of Public Administration, 43*(1), 850–865. https://doi.org/10.1080/01900692.2019.1660989

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

Coulter, K. S., & Coulter, R. A. (2003). The effects of industry knowledge on the development of trust in service relationships. *International Journal of Research in Marketing, 20*(1), 31–43. https://doi:10.1016/S0167-8116(02)00120-9

Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989). User acceptance of computer technology: A comparison of two theoretical models. *Management Science, 35*(8), 982–1003. https://www.jstor.org/stable/2632151

Faulkner, P. (2011). *The epistemology of testimony*: *Knowledge on trust.* Oxford University Press. https://doi:10.1093/acprof:oso/9780199589784.001.0001

Fung, S. (2023,July 7). *Cybercrime in Thailand: Current trends and solutions*. Pacific Prime Thailand. https://www.pacificprime.co.th/blog/cybercrime-thailand-trends/

Hair J. F., Jr., Howard, M. C., & Nitzl, C. (2020). Assessing measurement model quality in PLS-SEM using confirmatory. *Journal of Business Research*, *109*, 101–110. https://doi.org/10.1016/j.jbusres.2019.11.069

Hansen, J. M., Saridakis, G., & Benson, V. (2017). Risk, trust, and the interaction of perceived ease of use and behavioral control in predicting consumers' use of social media for transactions. *Computers in Human Behavior, 81,* 197–206. https//doi:10.1016/j.chb.2017.11.010

Humida, T., Mamun, M. B., & Keikhoscrokiani, P. (2021). Predicting behavioral intention to use e-learning system: A case-study in Begum Rokeya University, Rangpur, Bangladesh. *Education and Information Technologies, 27*(2), 2241–2265. https//doi:10.1007/s10639-021-10707-9

Hwang, J., Lee, J.-S., & Kim, H. (2019). Perceived innovativeness of drone food delivery services and its impacts on attitude and behavioral intentions: The moderating role of gender and age. *International Journal of Hospitality Management, 81*, 94–103. https//doi:10.1016/j.ijhm.2019.03.002

Karim, M.W., Haque, A., Ulfy, M. A., Hossain, M. A., & Anis, M. Z. (2020). Factors influencing the use of E-wallet as a payment method among Malaysian young adults. *Journal of International Business and Management, 3*(2), 1–12. https//doi:10.37227/jibm-2020-2-21

Kate, P. T. (2021, August 18). *Cyber attacks more than double since COVID-19, PwC Thailand says*. PwC Thailand. https://www.pwc.com/th/en/press-room/press-release/2021/press-release-18-08-21-en.html

Khoa, B. T. (2020). The impact of the personal data disclosure's tradeoff on the trust and attitude loyalty in mobile banking services. *Journal of Promotion Management, 27*(4), 585–608. https//doi:10.1080/10496491.2020.1838028

Kijsanayotin, B., Pannarunothai, S., & Speedie, S. M. (2009). Factors influencing health information technology adoption in Thailand's community health centers: Applying the UTAUT model. *International Journal of Medical Informatics, 78*(6), 404–416. https//doi:10.1016/j.ijmedinf.2008.12.005

Kim, R., & Song, HD (2022). Examining the influence of teaching presence and task-technology fit on continuance intention to use MOOCs. *The Asia-Pacific Education Researcher*, *31,* 395–408. https://doi.org/10.1007/s40299-021-00581-x

Kini, A., & Choobineh, J. (1998). Trust in electronic commerce: Definition and theoretical considerations. *Proceedings of the Thirty-First Hawaii International Conference on System Sciences*, *4*, 51–61. https//doi.org/10.1109/HICSS.1998.655251

Klerck, D., & Sweeney, J. C. (2007). Types on consumer-perceived risk and adoption of genetically modified foods. *Psychology and Marketing, 24*(2), 171–193. https//doi:10.1002/mar.20157

Kuo, YF, & Yen, SN (2009). Towards an understanding of the behavioral intention to use 3G mobile value-added services. *Computers in Human Behavior, 25*(1), 103–110. https://doi.org/10.1016/j.chb.2008.07.007

Liao, CH, Tsou, CW, & Huang, MF. (2007). Factors influencing the usage of 3G mobile services in Taiwan. *Online Information Review, 31*(6), 759–774. https://doi:10.1108/14684520710841757

Limbu, Y. B., Wolf, M., & Lusford, D. (2012). Perceived ethics of online retailers and consumer behavioral intentions: The mediating roles of trust and attitude. *Journal of Research in Interactive Marketing, 6(*2), 133–154. https://doi.org/10.1108/17505931211265435

Liu, P., Teng, M., & Han, C. (2020). How does environmental knowledge translate into pro-environmental behaviors?: The mediating role of environmental attitudes and behavioral intentions. *Science of the Total Environment, 728,* 138126. https://doi:10.1016/j.scitotenv.2020.138126

Mailizar, M., Burg, D., & Maulina, S. (2021). Examining university students' behavioural intention to use e-learning during the COVID-19 pandemic: An extended TAM model. *Education and Information Technologies, 26,* 7057–7077. https://doi:10.1007/s10639-021-10557-5

Minghao, P., & Wei, G. (2021). Determinants of the behavioral intention to use a mobile nursing application by nurses in China. *BMC Health Services Research, 21,* 228. https://doi:10.1186/s12913-021-06244-3

Morgan, S. (2020, November 13). *Cybercrime to cost the world $10.5 trillion annually by 2025*. Cybercrime Magazine. https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/

Mortensen, M., & Neeley, T. B. (2012). Reflected knowledge and trust in global collaboration. *Management Science, 58*, 2207–2224. https://:10.2307/23359587

National Cyber Security Agency (NCSA). (2023). *Annual Report 2022.* https://www.dlt.go.th/web-upload/1xff0d34e409a13ef56eea54c52a291126/filecenter/admin_admin.k/cybersec/Annual%20Report%20NCSA%202022.pdf

National Institute of Standards and Technology (NIST). (2018). *Framework for improving critical infrastructure cybersecurity.* https://doi.org/10.6028/NIST.CSWP.04162018

Park, C. W., Gardner, M. P., & Thukral, V. K. (1987). Self-perceived knowledge: Some effects on information processing for a choice task. *The American Journal of Psychology 101*(3), 401–424. https://doi:10.2307/1423087

Sinclair, J., & Irani, T. (2013). Advocacy advertising for biotechnology: The effect of public accountability on corporate trust and attitude toward the ad. *Journal of Advertising, 34*(3), 59–73. https://doi:10.1080/00913367.2005.10639203

Sukendro, S., Habibi, A., Khaeruddin, K., Indrayana, B., Syahruddin, S., Makadada, F. A., & Hakim, H. (2020). Using an extended technology acceptance model to understand students' use of e-learning during Covid-19: Indonesian sport science education context. *Heliyon,* 6(11), e05410. https://doi: 10.1016/j.heliyon.2020.e05410

The Economist. (2017, May 6). *The world's most valuable resource is no longer oil, but data*. https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data

Trumbo, C. W. (1999). Heuristic-systematic information processing and risk judgment. *Risk Analysis, 19*(3), 391–400. https://doi: 10.1023/a:1007092410720

Trumbo, C. W., & McComas, K. A. (2003). The function of credibility in information processing for risk perception. *Risk Analysis, 23*(2), 343–53. https://doi: 10.1111/1539-6924.00313

Zhu, W., Wei, J., & Zhao, D. (2016). Anti-nuclear behavioral intentions: The role of perceived knowledge, information processing, and risk perception. *Energy Policy, 88*, 168–177. https://doi.org/10.1016/j.enpol.2015.10.009

Zywiolek, J., Rosak-Szyrocka, J., Khan, M. A., & Sharif, A. (2022). Trust in renewable energy as part of energy-saving knowledge. *Energies, 15*(4), 1566. https://doi:10.3390/en15041566