Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 4, 2018-2028
2025
Publisher: Learning Gate
DOI: 10.55214/25768484.v9i4.6448

Cybersecurity readiness in Thailand: The empirical evidence of service sectors

Porramin Photipatphiboon[1], Thanuset Chokpiriyawat[2*], Kanokwan Papamo[3]
[1]Faculty of Business Administration, Sripatum University Khon Kaen Campus, Khon Kaen, Thailand.
[2,3]Faculty of Business Administration and Accountancy, Khon Kaen University, Khon Kaen, Thailand;
Thanuset.c@kkumail.com (T.C.)

Abstract: This study evaluates the cybersecurity maturity of Thailand's service sectors amid digital transformation. As advanced technologies become increasingly adopted in industries such as healthcare, education, tourism, and finance, these sectors encounter significant cybersecurity challenges due to the sensitivity of customer data and system interconnectivity. Utilizing the Technology, Organization, and Environment (TOE) framework, the study assesses cybersecurity readiness concerning technological, organizational, and environmental factors. Data were collected from 400 respondents through purposive sampling, and structural equation modeling (SEM) was employed for analysis. The study finds that technological, organizational, and environmental readiness significantly influence cybersecurity awareness. Among these, environmental readiness emerged as the most impactful, with external pressures like regulatory compliance and market competition shaping cybersecurity preparedness. Additionally, cybersecurity awareness strongly affects compliance behavior and the willingness to share cybersecurity knowledge within organizations. Cybersecurity awareness is crucial for improving compliance with security protocols and fostering a proactive cybersecurity culture. Strengthening awareness and preparedness across technological, organizational, and environmental levels is essential for effectively managing cybersecurity risks in service sectors undergoing digital transformation. The findings underscore the need for tailored cybersecurity policies and targeted training programs to build resilience against cyber threats, particularly in developing economies. The proposed framework and quantifiable index provide a practical tool for organizations to assess and improve cybersecurity readiness, ensuring better protection of sensitive data and regulatory compliance.

Keywords: *Cybersecurity maturity, Digital transformation, Service sectors, TOE framework.*

1. Introduction

The service industry is undergoing a significant transformation due to the rapid advancements in digital technology [1]. This shift has dramatically enhanced customer service, improved operational efficiency, and enabled data-driven decision-making [2]. Technological disruption has exposed customer data and critical systems to substantial cybersecurity risks [3]. The sensitive nature of customer information, combined with the increasing interconnectivity of digital systems, makes service sectors, including healthcare, finance, and retail, prime targets for cyberattacks. Such breaches can lead to severe financial losses and other significant disadvantages for organizations [4-6]. Cyberattacks often result in immediate financial setbacks and long-lasting harm to the company's brand and customer trust [7]. Furthermore, failing to invest in cybersecurity can impede a company's innovation or growth, as businesses may face higher operational costs, legal expenses, and increased insurance premiums after a breach. These challenges can slow growth and erode a company's competitiveness in the marketplace [8-10].

History: Received: 22 February 2025; Revised: 10 April 2025; Accepted: 14 April 2025; Published: 21 April 2025
* Correspondence: Thanuset.c@kkumail.com

While digital transformation presents numerous benefits, it also introduces complex cybersecurity challenges that many service organizations are ill-equipped to handle due to a lack of standardized cybersecurity readiness, limited resources, outdated systems, and insufficient staff training, contributing to a vulnerability gap that cyber threats can exploit [11]. Service organizations, in particular, face difficulties in assessing their cybersecurity readiness. Despite the critical importance of cybersecurity in service sectors, many organizations continue to adopt new digital technologies without adequately addressing the cybersecurity risks associated with these advancements. Inadequate cybersecurity preparedness within service sectors significantly compromises customer privacy, undermines operational safety, and jeopardizes the continuity of critical service delivery [12]. This situation highlights the need for a systematic approach to evaluate and enhance cybersecurity readiness in service organizations undergoing digital transformation [13]. Existing studies often focus on technical solutions or individual cyber incidents; however, there remains a significant gap in research providing a comprehensive and practical framework for assessing cybersecurity readiness within the context of the digital transformation of service sectors [14, 15].

The Technology, Organization, and Environment (TOE) framework can help reveal these gaps by providing a structured lens to assess the interplay of technological, organizational, and environmental factors in cybersecurity readiness [16, 17]. Organizations can evaluate their technological infrastructure, organizational processes, and external regulatory pressures while addressing the human element, ultimately enabling a more holistic and adaptive framework for managing cybersecurity risks in the rapidly evolving service sector. The research contributes significantly by offering two key insights into improving cybersecurity in service sectors. First, it proposes a comprehensive cybersecurity readiness framework integrating the TOE dimensions. This integrated approach allows service organizations to assess cybersecurity risks from a multi-dimensional perspective, encompassing technological, organizational, and environmental factors. Second, the study introduces a quantifiable cybersecurity readiness index for service sectors. This index assists organizations in evaluating their cybersecurity capabilities, identifying critical gaps, and prioritizing initiatives to strengthen their readiness. The study supports service sectors in developing countries or those facing resource constraints in better managing their cybersecurity challenges amid the digital transformation. The conceptual framework is illustrated in Figure 1.

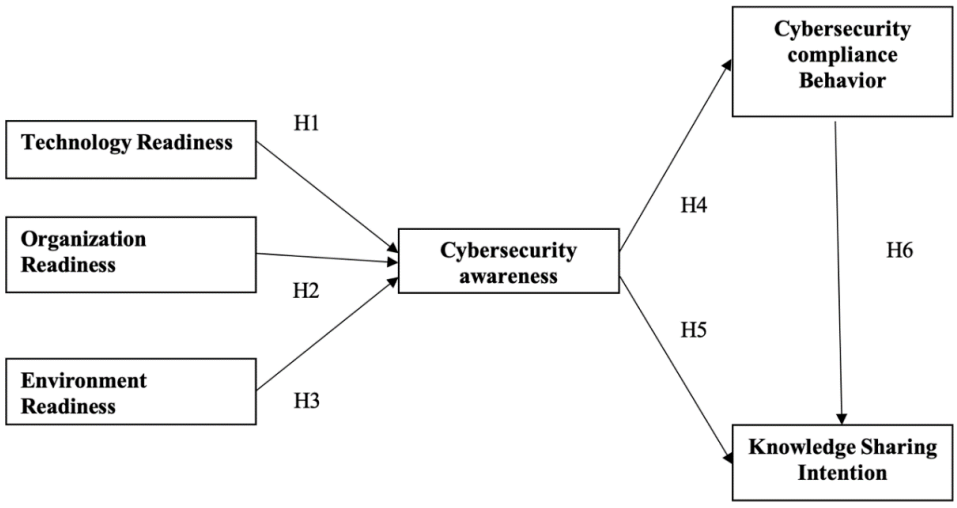

Figure 1.
Conceptual Framework.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 4: 2018-2028, 2025
DOI: 10.55214/25768484.v9i4.6448

2. Literature Review

2.1. TOE Framework

The technology-organization-environment (TOE) framework offers a multidimensional perspective for examining behavioral intentions and systemic adoption dynamics across diverse sectors [18, 19]. Organizations can systematically address the factors influencing adoption by incorporating the TOE framework in developing and implementing cybersecurity awareness programs. Technology readiness, an organization's preparedness and capacity to adopt and utilize emerging technologies, is essential for promoting cybersecurity awareness. Technologically advanced organizations are more likely to establish robust cybersecurity infrastructures and implement awareness programs that educate employees about threats and best practices [20, 21]. Furthermore, organizations implementing cybersecurity protocols significantly enhance their technological proficiency by systematically integrating cybersecurity measures into their digital strategies. This process embeds security awareness within routine operational practices and optimizes overall organizational efficiency [22]. Consequently, organizations with higher technological readiness are strategically positioned and strongly motivated to invest in targeted initiatives that heighten cybersecurity awareness, significantly deepening employees' understanding of cybersecurity risks and reinforcing secure behavioral compliance. The H1 is formed.

Hypothesis 1: Technology readiness impacts cybersecurity awareness.

Organizational readiness, characterized by leadership support, organizational culture, structural alignment, and resource allocation, significantly influences employees' cybersecurity awareness [23, 24]. Proactive leadership: A clear strategic direction in organizational readiness effectively enhances cybersecurity. Awareness can be achieved by aligning organizational policies, structured training programs, and robust internal communication channels, strengthening employee vigilance and responsiveness to cyber threats [15, 25]. Cybersecurity awareness is a function of technical tools and institutional commitment to cybersecurity values [26]. An organization's structural and cultural dimensions directly shape how cybersecurity is understood and internalized across its workforce [27, 28]. The H2 is formed.

Hypothesis 2: Organizational readiness impacts cybersecurity awareness.

Environmental readiness encompasses external pressures and support systems influencing an organization's cybersecurity posture [20]. Companies operating within highly regulated or intensely competitive environments tend to strengthen cybersecurity awareness initiatives to meet compliance requirements and mitigate reputational risks [29-31]. Cybersecurity education, awareness, and training are increasing, and governmental policies often stimulate awareness programs, urging organizations to educate their workforce on best practices [32]. Moreover, collaboration with security-conscious partners and clients enhances internal cybersecurity awareness efforts, as these external influences foster a sense of urgency and accountability, prompting organizations toward proactive security education and practices [33]. The H3 is formed.

Hypothesis 3: Environmental readiness impacts cybersecurity awareness.

2.2. Cybersecurity

Cybersecurity has become a paramount organizational priority in the digital age, propelled by the escalating frequency and complexity of cyber threats exploiting technological infrastructure and human vulnerabilities. Table 1 reviews previous cybersecurity.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 4: 2018-2028, 2025
DOI: 10.55214/25768484.v9i4.6448

Table 1.
Literature Review of Cybersecurity.

Source	Purpose	Sectors	Main result
Humaidi and Balakrishnan [34]	Identify factors influence compliance behavior	Health service	Management support of knowledge to employees boost both their self-efficiency and develop the level of company trust which impact to information security compliance behavior.
Tran, et al. [35]	Investigate the factors impact employees' behavior to protect organizational cybersecurity	Cooperated enterprise	Policies and security education, training and awareness program provided by corporate are associated with cybersecurity awareness which play important roles to attitude and intention promoting across cybersecurity.
Klein, et al. [36]	Compare cybersecurity behavior across regions	IT services	Awareness levels directly influence secure behavior; regional differences highlight the importance of tailored training.
Alahmari, et al. [37]	Explore knowledge-sharing beyond awareness	Financial services	Knowledge sharing is influenced by awareness, trust, and organizational support; compliance behavior enhances safe information exchange.
Pham, et al. [38]	Assess the effect of knowledge-sharing methods on security behavior	IT services	Secure knowledge-sharing practices improve cyber hygiene and awareness among staff.
Yusuf [39]	Explore awareness and compliance behavior	Higher education	Higher cybersecurity awareness significantly improves compliance behavior and reduces policy violations.
Zwilling, et al. [40]	Study awareness and behavior relationships	Professional services	Security awareness campaigns significantly shape employee behavior, especially among IT professionals.
TamjidYamcholo and Toloie Eshlaghy [41]	Investigate knowledge-sharing intention under compliance	Public services	Self-efficacy and perceived reciprocity enhance knowledge sharing within security-compliant environments.
Alsmadi, et al. [42]	Understand proactive behavior during crises	E-services	Awareness leads to proactive behavior; behavioral intention is shaped by security knowledge and system trust.
Muraguri, et al. [21]	Identify cybersecurity readiness enablers	Financial cooperatives	Technology and organization readiness strongly impact cybersecurity awareness and compliance culture.

The multidimensional approach to cybersecurity encompasses technological solutions, organizational strategies, policy compliance, and user behavior [43, 44]. Cybersecurity is not solely a technical issue; it is also deeply rooted in human factors such as awareness, behavior, and culture [45]. Thus, cybersecurity awareness is crucial for shaping employees' compliance with organizational security policies and procedures. Building sustained awareness is a strategic imperative to ensure security behavior aligns with policy expectations. The H4-5 are formed.

Hypothesis 4: Cybersecurity awareness impacts cybersecurity compliance behavior.

Hypothesis 5: Cybersecurity awareness impacts knowledge sharing intention.

Cybersecurity compliance behavior can significantly influence the intention to share knowledge by creating a secure, trustworthy environment where individuals feel confident exchanging information [32, 35, 46]. Employees who adhere to cybersecurity policies contribute to a culture of accountability and risk awareness that promotes safe knowledge dissemination. People adhering to cybersecurity compliances tend to place greater importance on secure collaboration, making them more likely to engage in responsible knowledge sharing [47, 48].

High-efficiency compliance behaviors reduce uncertainty regarding data misuse, reinforcing perceptions that shared information will be managed appropriately [49, 50]. Moreover, organizations

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 4: 2018-2028, 2025
DOI: 10.55214/25768484.v9i4.6448

with high compliance maturity often establish systems and norms that enhance security and encourage collaborative knowledge practices. Therefore, cybersecurity compliance enables intentional and cautious knowledge exchange by ensuring knowledge sharing occurs within a secure behavioral framework. The H6 is formed.

Hypothesis 6: Cybersecurity compliance behavior impacts knowledge-sharing intention.

3. Methodology

The methodology employed in this study utilizes a purposive sampling method with a quota of 461 respondents, employees with at least one year in the organization. Before completing the questionnaire, respondents will receive a comprehensive overview of the definition of research and the scope of cybersecurity within the context of this study. The unintentional respondents will be excluded by verifying when they begin and finish the questionnaire and asking them to type the survey's start and end times. Discrepancies between the starting and finishing times significantly lower than 15 minutes will result in exclusion from the study as part of the first screening of data robustness. A subsequent data cleaning round will analyze each construct's mean and standard deviation. The exclusion criteria were respondents whose answers deviated by more than 0.25 standard deviations from the study's established norms would be excluded [51]. Four hundred valid responses will be retained for further analysis, which includes measurement model evaluation and hypothesis testing. The questionnaire was adapted from prior studies to ensure relevance and validity within the research scope. Three items of technological readiness, three items of organization readiness, and three items of environmental readiness were adapted [20]. Four items of Cybersecurity Awareness were adapted from [52]. Three items of cybersecurity compliance behavior were adapted from [58]. Knowledge sharing intention adapted from Chokpiriyawat and Siriyota [10]. Data analysis will be conducted using SMART PLS 4.1.1.1 for measurement model, path analysis, and hypothesis testing.

4. Results

4.1. Sample Characteristics

The demographic profile of the sample group (n=400) demonstrates the highest number of respondents in Education (33.5%), followed by Tourism (27.0%), Healthcare (24.7%), and Financial Services (14.8%). Gender distribution reveals a predominance of female respondents (70.8%), with male participants representing 18.8% and LGBTQ+ individuals comprising 10.5%. Regarding education, most participants are undergraduate students (56.3%), with graduate students accounting for 25.3% and 18.5% categorized as Others, including those who did not wish to disclose their educational background or belong to other subcategories. The details are shown in Table 3.

Table 2.
Sample Characteristic.

Description	Number (n)	Percentage (%)
Service organization		
Tourism	108	27.0
Education	134	33.5
Healthcare	99	24.7
Financial	59	14.8
Gender		
Male	75	18.8
Female	283	70.8
LGBTQ+	42	10.5
Education		
Undergraduate	225	56.3
Graduate	101	25.3
Others	74	18.5
Total	400	100

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 4: 2018-2028, 2025
DOI: 10.55214/25768484.v9i4.6448

4.2. Measurement Model

All six constructs exhibit excellent internal consistency, with Cronbach's Alpha values ranging from 0.877 to 0.943, well above the 0.7 threshold. Convergent validity is also confirmed, with Average Variance Extracted (AVE) values between 0.842 and 0.898, indicating that the items within each construct effectively capture the underlying dimensions [53]. Composite Reliability (CR) values ranging from 0.953 to 0.964 further support the robustness of the measurement model. Factor loadings consistently exceed 0.922, reinforcing the validity of the constructs. Additionally, Variance Inflation Factor (VIF) values remain below the critical threshold of 5, indicating no issues with multicollinearity [54]. The constructs exhibit high reliability, validity, and consistency, ensuring their robustness for subsequent analysis, as shown in Table 3.

Table 3.
Measurement model.

Items	Loading	VIF	CR	AVE	Cronbach's alpha
Technological Readiness			0.954	0.874	0.928
(TC1) Your organization has IT cybersecurity experts who meet standards in terms of efficiency and numbers.	0.927	3.464			
(TC2) Your organization has sufficient tools and equipment for effective cyber security management.	0.946	4.263			
(TC3) Your organization has invested in its own technology to manage cyber security adequately and efficiently.	0.931	3.506			
Organization Readiness			0.964	0.898	0.943
(OC1) Your organization has cybersecurity experts on staff.	0.951	4.762			
(OC2) Your organization provides training workshops and activities that promote the development of personnel responsible for cybersecurity.	0.949	4.637			
(OC3) Your organization has the human resources to manage cyber security.	0.944	4.193			
Environmental Readiness			0.955	0.877	0.930
(EC1) Your organization is making efforts to communicate with all relevant departments to ensure that cybersecurity activities run smoothly.	0.927	3.367			
(EC2) Cybersecurity is continuously improved across all relevant functions across the organization.	0.942	4.061			
(EC3) Your organization has managed knowledge from experience to ensure that it can solve problems that arise within the organization.	0.941	3.999			
Cybersecurity Awareness			.955	.842	.937
(AW1) You have concerns about cyber security	0.922	3.968			
(AW2) You know someone who is in charge of cyber security.	0.898	3.125			
(AW3) You understand the risks that can arise if cybersecurity is not maintained.	0.921	3.853			
(AW4) You are aware of the serious threats that can arise if there is no cybersecurity.	0.929	4.354			
Cybersecurity Compliance Behavior			0.953	0.966	0.877
(COM1) You are committed to cyber security.	0.946	4.602			
(COM2) You are confident that you are complying with cyber security guidelines.	0.930	4.419			
(COM3) You intend to comply with any future cybersecurity regulations that may be introduced.	0.933	4.461			
(COM4) You intend to attend any future cybersecurity training.	0.945	4.876			
Knowledge Sharing Intention			0.962	0.894	0.941
(KSI1) You will tell your friends and family about the best practices for cyber security.	0.939	3.913			
(KSI2) When cybersecurity is mentioned in a conversation, you intend to share your knowledge.	0.950	4.671			
(KSI3) You will be able to provide cybersecurity advice when someone you know asks you for advice.	0.948	4.530			

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 4: 2018-2028, 2025
DOI: 10.55214/25768484.v9i4.6448

4.3. Hypothesis Testing and Path Analysis

Partial Least Squares Structural Equation Modeling (PLS-SEM) using SmartPLS 4.1.1 After assessing the measurement model for reliability and validity, we start evaluating the structural model through path analysis. Path coefficients, R^2 values, and predictive relevance (Q^2) are analyzed to determine the model's predictive accuracy and significance of relationships. A bootstrapping procedure with 10,000 samples and bias-corrected confidence intervals (BCa) is used to test hypotheses. The results provide insights into the model's explanatory power, predictive relevance, and theoretical contributions in Figure 2.

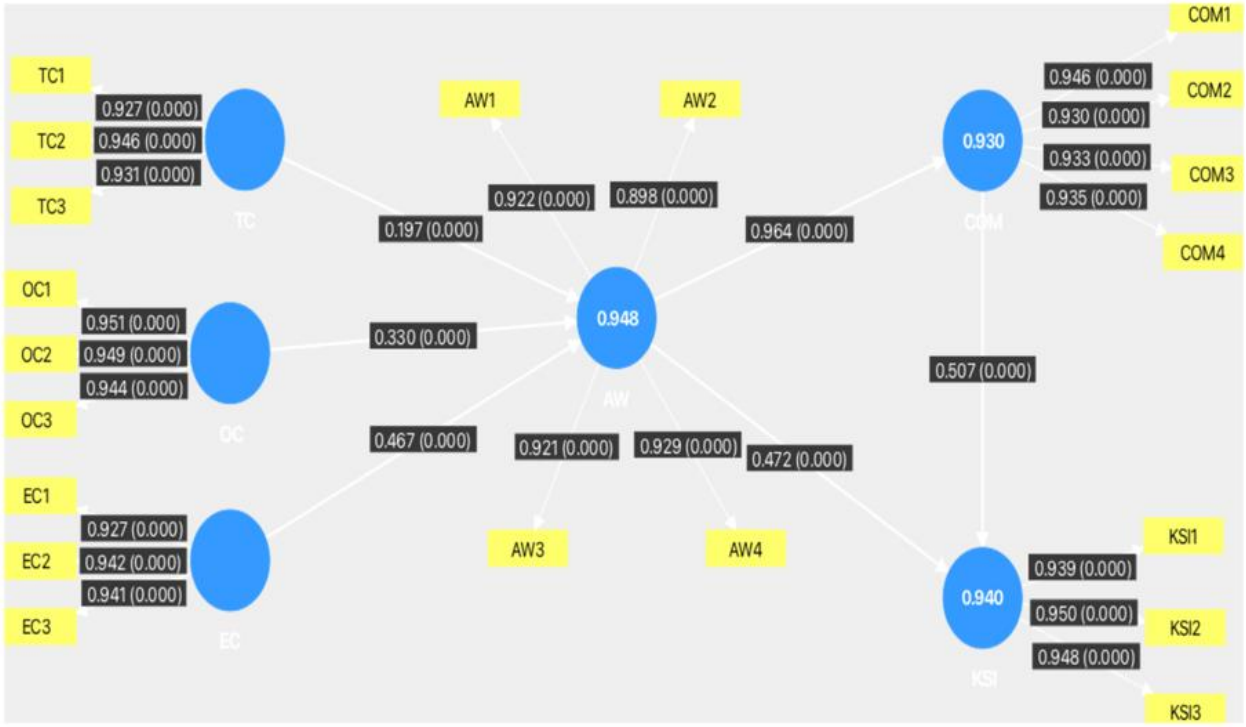

Figure 2.
Path Analysis and Hypothesis Testing.

Table 4 presents the path coefficients, standard deviations, t-statistics, p-values, R^2, and Q^2 values. All six hypothesized relationships were supported. The relationship between technological readiness and cybersecurity awareness was significant ($\beta = 0.197$, $t = 3.908$, $p < 0.001$). The model explained 94.8% of the variance in cybersecurity awareness ($R^2 = 0.948$), and the Q^2 value was 0.946, indicating good predictive validity. Therefore, hypothesis 1 was supported. The relationship between Organizational Readiness and Cybersecurity Awareness was also significant ($\beta = 0.330$, $t = 7.231$, $p < 0.001$), with a substantial effect size. The p-value indicates that the relationship is statistically significant. Hypothesis 2 was supported. Environmental readiness positively impacted cybersecurity awareness ($\beta = 0.467$, $t = 8.536$, $p < 0.001$), indicating a strong influence of environmental factors on cybersecurity awareness. Hypothesis 3 was supported. Cybersecurity awareness strongly and positively affected cybersecurity compliance behavior ($\beta = 0.964$, $t = 227.186$, $p < 0.001$). The R^2 value was 0.930, indicating that cybersecurity awareness explains a significant portion of the variance in cybersecurity compliance behavior. The Q^2 value was 0.939, confirming the model's predictive capability [55] and supporting hypothesis 4. The relationship between cybersecurity awareness and knowledge-sharing intention was significant ($\beta = 0.472$, $t = 6.650$, $p < 0.001$), suggesting that higher cybersecurity

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 4: 2018-2028, 2025
DOI: 10.55214/25768484.v9i4.6448

awareness increases the intention to share knowledge, thereby supporting hypothesis 5. Cybersecurity compliance behavior positively influenced knowledge-sharing intention ($\beta = 0.507$, $t = 7.158$, $p < 0.001$). This relationship was also statistically significant, indicating that compliance with cybersecurity practices encourages knowledge sharing, thus supporting hypothesis 6. The results suggest that technological readiness, organizational readiness, and environmental readiness positively influence cybersecurity awareness, which, in turn, significantly impacts both cybersecurity compliance behavior and knowledge-sharing intention. The model demonstrated high explanatory power, with R^2 values above 0. 0.9 for all key relationships and strong predictive validity, as indicated by the Q^2 values.

Table 4.
Hypothesis Testing, Path Analysis, R^2, and Q^2.

Relationship	Path Coefficient	Standard Deviation	t- Statistics	P-value	R^2	Q^2	Interpretation
H1: TR > CA	0.197	0.050	3.908	0.000	0.948	0.946	Supported
H2: OR > CA	0.330	0.046	7.231	0.000			Supported
H3: ER > CA	0.467	0.055	8.536	0.000			Supported
H4: CA > CCB	0.964	0.004	227.186	0.000	0.930	0.939	Supported
H5: CA> KSI	0.472	0.071	6.650	0.000	0.940	0.911	Supported
H6: CCB> KSI	0.507	0.071	7.158	0.000			Supported

5. Conclusion

The findings provide significant insights into the interconnections among the TOE Framework of readiness, cybersecurity awareness, cybersecurity compliance behavior, and knowledge-sharing intention. The study emphasizes the importance of organizational readiness and sector-specific factors in influencing these relationships, highlighting the need for tailored cybersecurity training and policy implementation approaches. Organizations can better manage risk and foster a culture of collaboration and knowledge sharing by understanding the factors that influence cybersecurity behavior.

The findings of this study emphasize the critical need for tailored cybersecurity policies and comprehensive training programs that can enhance resilience against cyber threats, particularly within developing economies. Service organizations in Thailand, and similar regions undergoing digital transformation, must prioritize strengthening cybersecurity at the technological, organizational, and environmental levels. By adopting the proposed framework, companies can assess and improve their cybersecurity readiness, ensuring better protection of sensitive customer data and ensuring compliance with evolving regulatory standards. This approach not only mitigates risks but also fosters a culture of proactive cybersecurity, which is crucial for long-term business success.

Future research should extend this study by exploring cybersecurity maturity in other sectors beyond the service industry, such as manufacturing and retail, to gain broader insights into industry-specific challenges. Additionally, more in-depth qualitative research could be conducted to understand the barriers organizations face in implementing cybersecurity strategies. Future studies could also explore the impact of emerging technologies, like AI and machine learning, on cybersecurity preparedness and resilience. Another avenue for future investigation is the role of government regulations and public policy in shaping organizational approaches to cybersecurity, particularly in developing countries where regulatory frameworks may still be evolving.

Transparency:

The authors confirm that the manuscript is an honest, accurate, and transparent account of the study; that no vital features of the study have been omitted; and that any discrepancies from the study as planned have been explained. This study followed all ethical practices during writing.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 4: 2018-2028, 2025
DOI: 10.55214/25768484.v9i4.6448

References
[1] M. Zaki, "Digital transformation: Harnessing digital technologies for the next generation of services," *Journal of Services Marketing*, vol. 33, no. 4, pp. 429-435, 2019. https://doi.org/10.1108/JSM-01-2019-0034
[2] A. Bousdekis, K. Lepenioti, D. Apostolou, and G. Mentzas, "A review of data-driven decision-making methods for industry 4.0 maintenance applications," *Electronics*, vol. 10, no. 7, p. 828, 2021. https://doi.org/10.3390/electronics10070828
[3] T. Limba, A. Stankevičius, and A. Andrulevičius, "Industry 4.0 and national security: the phenomenon of disruptive technology," *Journal of Engineering Sciences and Innovation*, vol. 6, no. 3, pp. 1528–1535, 2019. https://doi.org/10.9770/jesi.2019.6.3(33)
[4] I. Lee, "Cybersecurity: Risk management framework and investment cost analysis," *Business Horizons*, vol. 64, no. 5, pp. 659-671, 2021. https://doi.org/10.1016/j.bushor.2021.02.022
[5] M. H. U. Sharif and M. A. Mohammed, "A literature review of financial losses statistics for cyber security and future trend," *World Journal of Advanced Research and Reviews*, vol. 15, no. 1, pp. 138-156, 2022. https://doi.org/10.30574/wjarr.2022.15.1.0573
[6] P. V. Shevchenko, J. Jang, M. Malavasi, G. W. Peters, G. Sofronov, and S. Trück, "The nature of losses from cyber-related events: risk categories and business sectors," *Journal of Cybersecurity*, vol. 9, no. 1, p. tyac016, 2023. https://doi.org/10.1093/cybsec/tyac016
[7] K. A. Whitler and P. W. Farris, "The impact of cyber attacks on brand image: Why proactive marketing expertise is needed for managing data breaches," *Journal of Advertising Research*, vol. 57, no. 1, pp. 3-9, 2017. https://doi.org/10.2501/JAR-2017-005
[8] D. Kosutic and F. Pigni, "Cybersecurity: investing for competitive outcomes," *Journal of Business Strategy*, vol. 43, no. 1, pp. 28-36, 2022. https://doi.org/10.1108/JBS-06-2020-0116
[9] G. Tsankova, "Enterprise security as an element of market competitiveness," *Educational and Scientific Policy Strategies*, vol. 32, no. 1s, pp. 98-107, 2024. https://doi.org/10.53656/str2024-1s-7-ent
[10] T. Chokpiriyawat and K. Siriyota, "The impact of service recovery actions and perceived justice on customer satisfaction: Insights from Thailand's private hospitals," *International Journal of Analysis and Applications*, vol. 22, pp. 81-81, 2024.
[11] S. Starke, I. Ludviga, and J. Fröhlich, "Ability, motivation and opportunity to participate in the digital change: A focus group study on new concepts for sustained learning in healthcare organisations," *Edelweiss Applied Science and Technology*, vol. 9, no. 3, pp. 61-74, 2025. https://doi.org/10.55214/25768484.v9i3.5114
[12] G. Lykou, A. Anagnostopoulou, and D. Gritzalis, "Smart airport cybersecurity: Threat mitigation and cyber resilience controls," *Sensors*, vol. 19, no. 1, p. 19, 2018. https://doi.org/10.3390/s19010019
[13] A. Folorunso, I. Wada, B. Samuel, and V. Mohammed, "Security compliance and its implication for cybersecurity," *World Journal of Advanced Research and Reviews*, vol. 24, no. 01, pp. 2105-2121, 2024. https://doi.org/10.30574/wjarr.2024.24.1.3170
[14] S. Hasan, M. Ali, S. Kurnia, and R. Thurasamy, "Evaluating the cyber security readiness of organizations and its influence on performance," *Journal of Information Security and Applications*, vol. 58, p. 102726, 2021. https://doi.org/10.1016/j.jisa.2020.102726
[15] M. Neri, F. Niccolini, and L. Martino, "Organizational cybersecurity readiness in the ICT sector: A quanti-qualitative assessment," *Information & Computer Security*, vol. 32, no. 1, pp. 38-52, 2024. https://doi.org/10.1108/ICS-05-2023-0084
[16] A. Marei, "An empirical study on the impact of TOE factors on e-accounting adoption: The moderating role of cybersecurity," *Journal of Strategic Marketing and Services*, vol. 14, no. 3, pp. 266–292, 2024. https://doi.org/10.33168/JSMS.2024.0316
[17] T. Hasani, N. O'Reilly, A. Dehghantanha, D. Rezania, and N. Levallet, "Evaluating the adoption of cybersecurity and its influence on organizational performance," *SN Business & Economics*, vol. 3, no. 5, p. 97, 2023. https://doi.org/10.1007/s43546-023-00477-6
[18] S. C. Eze, V. C. Chinedu-Eze, H. O. Awa, and T. A. Asiyanbola, "Multi-dimensional framework of the information behaviour of SMEs on emerging information communication technology (EICT) adoption," *Journal of Science and Technology Policy Management*, vol. 14, no. 6, pp. 1006-1036, 2023. https://doi.org/10.1108/JSTPM-11-2021-0172
[19] S. Malik, M. Chadhar, S. Vatanasakdakul, and M. Chetty, "Factors affecting the organizational adoption of blockchain technology: Extending the technology–organization–environment (TOE) framework in the Australian context," *Sustainability*, vol. 13, no. 16, p. 9404, 2021. https://doi.org/10.3390/su13169404

[20] Berlilana, T. Noparumpa, A. Ruangkanjanases, T. Hariguna, and Sarmini, "Organization benefit as an outcome of organizational security adoption: The role of cyber security readiness and technology readiness," *Sustainability*, vol. 13, no. 24, p. 13761, 2021. https://doi.org/10.3390/su132413761

[21] N. Muraguri, T. Mwalili, and T. Mose, "Factors influencing cybersecurity readiness in deposit taking savings and credit cooperatives: A case study of Nairobi County," *International Academic Journal of Information Systems and Technology*, vol. 2, no. 1, pp. 157-182, 2019.

[22] A. Alzghoul and O. Al-kasasbeh, "The moderating role of information technology infrastructure in the relationship between fintech adoption and organizational competitiveness," *Investment Management & Financial Innovations*, vol. 21, no. 2, p. 155, 2024. https://doi.org/10.21511/imfi.21(2).2024.12

[23] S. Allahawiah, H. Altarawneh, and M. Al-Hajaya, "The role of organizational culture in cybersecurity readiness: An empirical study of the Jordanian Ministry of Justice," *Calitatea*, vol. 25, no. 202, pp. 74-84, 2024. https://doi.org/10.47750/QAS/25.202.08

[24] A. M. Asfahani, "Perceptions of organizational responsibility for cybersecurity in Saudi Arabia: A moderated mediation analysis," *International Journal of Information Security*, vol. 23, no. 4, pp. 2515-2530, 2024. https://doi.org/10.1007/s10207-024-00859-3

[25] L. A. Onyekwere, J. Nwokocha, and N. P. Ololube, "Proactive leadership and global transformation in organizational policy and management (OPM)." *International Journal of Institutional Leadership, Policy and Management*, vol. 1, no. 1, pp. 176-201, 2019.

[26] A. Georgiadou, S. Mouzakitis, K. Bounas, and D. Askounis, "A cyber-security culture framework for assessing organization readiness," *Journal of Computer Information Systems*, vol. 62, no. 3, pp. 452-462, 2022. https://doi.org/10.1080/08874417.2020.1845583

[27] E. Pavlova, "Enhancing the organisational culture related to cyber security during the university digital transformation," *Information & Security*, vol. 46, no. 3, pp. 239-249, 2020. https://doi.org/10.11610/isij.4617

[28] A. Sutton and L. Tompson, "Towards a cybersecurity culture-behaviour framework: A rapid evidence review," *Computers & Security*, vol. 148, p. 104110, 2024. https://doi.org/10.1016/j.cose.2024.104110

[29] S. Akter, M. R. Uddin, S. Sajib, W. J. T. Lee, K. Michael, and M. A. Hossain, "Reconceptualizing cybersecurity awareness capability in the data-driven digital economy," *Annals of Operations Research*, pp. 1-26, 2022. https://doi.org/10.1007/s10479-022-04844-8

[30] C. Z. Oroni and F. Xianping, "Structural evaluation of management capability and the mediation role of cybersecurity awareness towards enterprise performance," *Journal of Data, Information and Management*, vol. 5, no. 4, pp. 345-361, 2023. https://doi.org/10.1007/s42488-023-00108-7

[31] P. R. Trim and Y.-I. Lee, "The role of B2B marketers in increasing cyber security awareness and influencing behavioural change," *Industrial Marketing Management*, vol. 83, pp. 224-238, 2019. https://doi.org/10.1016/j.indmarman.2019.04.003

[32] R. Shillair, P. Esteve-González, W. H. Dutton, S. Creese, E. Nagyfejeo, and B. von Solms, "Cybersecurity education, awareness raising, and training initiatives: National level evidence-based results, challenges, and promise," *Computers & Security*, vol. 119, p. 102756, 2022. https://doi.org/10.1016/j.cose.2022.102756

[33] I. Krawczyk-Sokołowska and W. Caputa, "Awareness of network security and customer value–The company and customer perspective," *Technological Forecasting and Social Change*, vol. 190, p. 122430, 2023. https://doi.org/10.1016/j.techfore.2023.122430

[34] N. Humaidi and V. Balakrishnan, "Indirect effect of management support on users' compliance behaviour towards information security policies," *Health Information Management Journal*, vol. 47, no. 1, pp. 17-27, 2018. https://doi.org/10.1177/1833358317700255

[35] D. V. Tran, P. V. Nguyen, L. P. Le, and S. T. N. Nguyen, "From awareness to behaviour: understanding cybersecurity compliance in Vietnam," *International Journal of Organizational Analysis*, vol. 33, no. 1, pp. 209-229, 2025. https://doi.org/10.1108/IJOA-12-2023-4147

[36] G. Klein, M. Zwilling, and D. Lesjak, *A comparative study in israel and slovenia regarding the awareness, knowledge, and behavior regarding cyber security* (Research Anthology on Business Aspects of Cybersecurity). Hershey, PA: IGI Global, 2022.

[37] S. Alahmari, K. Renaud, and I. Omoronyia, "Moving beyond cyber security awareness and training to engendering security knowledge sharing," *Information Systems and e-Business Management*, vol. 21, no. 1, pp. 123-158, 2023. https://doi.org/10.1007/s10257-022-00500-4

[38] H. C. Pham, M. Nkhoma, and M. N. Nguyen, "Knowledge sharing and internal social marketing in improving cyber security practice," in *Cybersecurity, Privacy and Freedom Protection in the Connected World: Proceedings of the 13th International Conference on Global Security, Safety and Sustainability, London, January 2021, Springer*, 2021, pp. 431-439.

[39] A. A. Yusuf, "Employees' cybersecurity awareness and behaviour in South African higher education institutions," Master's Thesis, University of Pretoria (South Africa, 2024.

[40] M. Zwilling, G. Klien, D. Lesjak, Ł. Wiechetek, F. Cetin, and H. N. Basim, "Cyber security awareness, knowledge and behavior: A comparative study," *Journal of Computer Information Systems*, vol. 62, no. 1, pp. 82-97, 2022.

[41] A. TamjidYamcholo and A. Toloie Eshlaghy, "Subjectivity reduction of qualitative approach in information security risk analysis," *Journal of System Management*, vol. 8, no. 1, pp. 145-166, 2022.

[42] D. Alsmadi, A. Maqousi, and T. Abuhussein, "Engaging in cybersecurity proactive behavior: Awareness in COVID-19 age," *Kybernetes*, vol. 53, no. 1, pp. 451-466, 2024. https://doi.org/10.1108/K-08-2022-1104

[43] S. AlDaajeh and S. Alrabaee, "Strategic cybersecurity," *Computers & Security*, vol. 141, p. 103845, 2024. https://doi.org/10.1016/j.cose.2024.103845

[44] A. M. Al-Hawamleh, "Investigating the multifaceted dynamics of cybersecurity practices and their impact on the quality of e-government services: evidence from the KSA," *Digital Policy, Regulation and Governance*, vol. 26, no. 3, pp. 317-336, 2024. https://doi.org/10.1108/DPRG-11-2023-0168

[45] M. Hakimi, M. M. Quchi, and A. W. Fazil, "Human factors in cybersecurity: An in depth analysis of user centric studies," *Jurnal Ilmiah Multidisiplin Indonesia*, vol. 3, no. 01, pp. 20-33, 2024. https://doi.org/10.58471/esaprom.v3i01.3832

[46] A.-T. Delso-Vicente, L. Diaz-Marcos, O. Aguado-Tevar, and M. G. de Blanes-Sebastián, "Factors influencing employee compliance with information security policies: a systematic literature review of behavioral and technological aspects in cybersecurity," *Future Business Journal*, vol. 11, no. 1, p. 28, 2025. https://doi.org/10.1186/s43093-025-00452-7

[47] L.-W. Wong, V.-H. Lee, G. W.-H. Tan, K.-B. Ooi, and A. Sohal, "The role of cybersecurity and policy awareness in shifting employee compliance attitudes: Building supply chain capabilities," *International Journal of Information Management*, vol. 66, p. 102520, 2022. https://doi.org/10.1016/j.ijinfomgt.2022.102520

[48] H. C. Pham, I. Ulhaq, M. Nguyen, and M. Nkhoma, "An exploratory study of the effects of knowledge sharing methods on cyber security practice," *Australasian Journal of Information Systems*, vol. 25, 2021. https://doi.org/10.3127/ajis.v25i0.2177

[49] Y. T. Chua *et al.*, "Identifying unintended harms of cybersecurity countermeasures," in *2019 APWG Symposium on Electronic Crime Research (eCrime)*, 2019: IEEE, pp. 1-15.

[50] N. S. Sulaiman, M. A. Fauzi, W. Wider, J. Rajadurai, S. Hussain, and S. A. Harun, "Cyber–information security compliance and violation behaviour in organisations: A systematic review," *Social Sciences*, vol. 11, no. 9, p. 386, 2022. https://doi.org/10.3390/socsci11090386

[51] J. E. Collier, *Applied structural equation modeling using AMOS: Basic to advanced techniques*, 1st ed. New York: Routledge, 2020.

[52] F. Karlsson, M. Karlsson, and J. Åström, "Measuring employees' compliance–the importance of value pluralism," *Information & Computer Security*, vol. 25, no. 3, pp. 279-299, 2017. https://doi.org/10.1108/ICS-11-2016-0084

[53] J. F. Hair, *A primer on partial least squares structural equation modeling (PLS-SEM)*, 2nd ed. Los Angeles: Sage, 2017.

[54] C. Fornell and D. F. Larcker, "Evaluating structural equation models with unobservable variables and measurement error," *Journal of Marketing Research*, vol. 18, no. 1, pp. 39-50, 1981. https://doi.org/10.2307/3151312

[55] J. F. Hair Jr, M. C. Howard, and C. Nitzl, "Assessing measurement model quality in PLS-SEM using confirmatory composite analysis," *Journal of Business Research*, vol. 109, pp. 101-110, 2020. https://doi.org/10.1016/j.jbusres.2019.11.069

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 4: 2018-2028, 2025
DOI: 10.55214/25768484.v9i4.6448