JOURNAL OF SOCIAL TRANSFORMATION AND REGIONAL DEVELOPMENT
e-ISSN: 2682-9142

Vol. 7 No. 2 (2025) 52-72
https://publisher.uthm.edu.my/ojs/index.php/jstard

JSTARD

Mind The Risk: Exploring What Drives Cybersecurity Readiness Among Digital Consumers in Sarawak

Maximus Balla Tang[1]*, Jessica Lyn Andam[2], Mohd Ngah Ismail Suzali[3]

[1] *Centre for University Courses and Innovative Learning,*
University of Technology Sarawak, 96000 Sibu, Sarawak, MALAYSIA
[2] *School of Foundation Studies,*
University of Technology Sarawak, 96000 Sibu, Sarawak, MALAYSIA
[3] *Faculty of Economics and Business,*
Universiti Malaysia Sarawak, 94300 Kota Samarahan, Sarawak, MALAYSIA

*Corresponding Author: maximus@uts.edu.my
DOI: https://doi.org/10.30880/jstard.2025.07.02.006

Article Info

Received: 4 May 2025
Accepted: 10 October 2025
Available online: 1 December 2025

Keywords

Sarawak digital transformation; Unified Theory of Acceptance and Use of Technology (UTAUT); cybersecurity readiness; perceived risk; behavioural intention; cybersecurity awareness

Abstract

Sarawak is undergoing a significant digital transition with the aim of becoming a fully integrated and digitally driven economy by 2030. However, as digital device usage increases, consumers are confronted with a variety of cybersecurity concerns. The main objective of this research is to assess the psychological factors influencing digital consumers' readiness to engage with cybersecurity measures in Sarawak's digital transformation. To accomplish this, the study expands the Unified Theory of Acceptance and Use of Technology (UTAUT) model to provide a comprehensive framework to measure cybersecurity readiness. A quantitative research approach was employed, with a sample size of 400 respondents. The study employed SmartPLS 4.0 to conduct data analysis, utilizing its capabilities for Partial Least Squares Structural Equation Modeling (PLS-SEM). The study finds that six out of ten hypotheses were supported, with performance expectancy, facilitating conditions, perceived risk, and cybersecurity awareness significantly influencing consumers' behavioural intention to adopt cybersecurity measures. Additionally, behavioural intention and cybersecurity awareness were found to be significant factors in determining cybersecurity readiness. As Sarawak undergoes digital transformation, understanding the factors that affect cybersecurity readiness is crucial to ensure the population is prepared for the risks and challenges of new technologies. This study makes three key contributions: (1) It extends the UTAUT model by adding cybersecurity behaviours, offering a clearer understanding of digital consumers' cybersecurity readiness. (2) It offers valuable insights for policymakers in Sarawak. (3) The findings also provide valuable guidance for businesses to tailor their digital products and cybersecurity-related services to better meet the readiness levels and needs of consumers in Sarawak's evolving digital landscape.

1. Introduction

In the 21st century, digitalization has revolutionized the way businesses, governments, and individuals interact with information, data, and technology. Digital technologies like the Internet of Things (IoT), Artificial Intelligence

(AI), and Machine Learning (ML) are altering businesses and opening up new prospects for growth and innovation (Kumar et al., 2024). However, as consumers use digital devices more frequently in their daily lives, they encounter a range of cybersecurity concerns. The increasing reliance on internet services, digital transactions, and connected devices creates both convenience and risk. According to Garba and Bade (2021), any information stored in cyberspace including financial, military, government, and personal data is subject to cyberattack. Cybersecurity readiness has become an essential component of any digital project in today's interconnected world. According to Al-Fatlawi (2024), cybersecurity is a fundamental pillar that supports the stability, privacy, and trust that underpin modern society. The possibility of cyber threats grows tremendously as businesses and governments enhance their online presence and digitize services. Cybersecurity should be a priority for all internet users as borderless communication raises numerous security issues for consumers (Supayah & Ibrahim, 2016). As cyber threats grow, everyone must be aware, adaptable, and aggressive in order to guard against these ever-present hazards.

The Fourth Industrial Revolution (IR 4.0) represents a paradigm shift in the Malaysian economic landscape. As the Fourth Industrial Revolution (IR4.0) accelerates the integration of advanced technologies such as IoT, AI, and big data into daily life and business operations, ensuring cybersecurity readiness becomes increasingly critical to protect digital infrastructure and maintain user trust. The Malaysian government launched the Malaysia National Policy on IR 4.0 (Industry4RWD) which sought to push manufacturing industries towards IR 4.0 (Yong et al., 2020). The Malaysian government has been actively promoting the use of IR 4.0 technologies. IR 4.0 is the current phase of the industrial revolution that is heavily focused on real-time data, machine learning, automation, and interconnection (Sekak et al., 2022). The shift to IR 4.0 is reshaping not only manufacturing sectors but also service industries, agriculture, healthcare, and even government operations. Malaysia's dedication to creating a digital transformation-friendly ecosystem demonstrates its intention to become a regional digital leader (Khan et al., 2024). IR4.0 brings more digital technology into everyday life, making cybersecurity readiness more important to protect systems and users from growing online threats.

Building on Malaysia's commitment to fostering a digital transformation-friendly ecosystem, Sarawak is making notable strides in its own digital transition. Sarawak is currently undergoing a significant digital transition, guided by the aim of becoming a fully integrated and digitally driven economy by 2030. As Sarawak undergoes rapid digital transformation in line with IR4.0, cybersecurity readiness is essential to safeguard its expanding digital infrastructure and support sustainable technological growth. According to Hamarah and Mohamad (2020), the shift to the digital economy is the pioneering step in progressing the economy of Sarawak to avoid over-reliance on natural resources. The state administration implemented the Sarawak Digital Economy Strategy to reach high-income status through digital transformation (Jugah et al., 2022). The state administration unveiled the Sarawak Digital Economy (SDE) Blueprint 2030 which establishes a comprehensive framework to establish Sarawak as a digital hub in Southeast Asia (Sarawak Multimedia Authority, 2023). As Sarawak embraces digitalization, the increase in cybercrime poses a growing risk to the state's digital economy, businesses, and citizens.

This study aims to assess the psychological factors influencing digital consumers' readiness to engage with cybersecurity measures in Sarawak's digital transformation. This study is significant because, as Sarawak advances its digital transformation under the IR4.0 agenda, the success of these initiatives relies not only on technological infrastructure but also on the public's readiness to adopt safe and secure digital practices. There is a growing body of research on cybersecurity across different sectors and populations (Hakiem et al., 2023; Hasan et al., 2021; Neri et al., 2023). However, there is limited research on how these factors interact and influence cybersecurity readiness specifically within the context of Sarawak's digital transformation. Hence, there is a significant gap in research that examines how these factors collectively influence consumers' readiness to engage with cybersecurity measures in Sarawak. A deeper understanding of the factors that shape consumer perspectives on cybersecurity readiness is required. Understanding how performance expectancy, effort expectancy, social influence, facilitating conditions, perceived risk, and cybersecurity awareness interact can help policymakers, businesses, and digital service providers design more effective strategies to enhance consumer engagement with cybersecurity.

The rest of this article is structured as follows: Section 2 reviews the relevant literature, discusses hypothesis development, and outlines the conceptual framework. Section 3 details the research methodology which includes research design, sampling methods and data analysis techniques. In Section 4, we present the empirical results and discussion. Finally, Section 5 offers the concluding remarks.

2. Literature Review

2.1 Definition of Cybersecurity

As the digital age progresses, cybersecurity has evolved into an essential component of individual, organizational, and governmental operations. According to Seemma et al. (2019), cybersecurity can be defined as the endeavour to protect a user's or organization's cyberenvironment. The expansion of the internet and greater reliance on digital technology across industries have created both opportunities and challenges. According to Kalakuntla et al., (2019), cybersecurity refers to safeguarding data in the area of data technology. At its foundation, cybersecurity seeks to ensure the confidentiality, integrity, and availability of information and resources in the digital realm. Taherdoost (2022) further defined cybersecurity as the process of protecting information from cyber dangers and cyberattacks while it is processed, stored, or transmitted. Cybersecurity is critical for protecting sensitive data and ensuring the operation of critical services in today's interconnected world. Cybersecurity is security in the cyber world to protect from the exploitation of sensitive and vital information (Kazemi et al., 2023). In this study context, cybersecurity is the activity of securing systems, networks, and digital data from unwanted access, theft, damage, or interruption.

2.2 Sarawak’s Digital Transformation

Sarawak is embarking on a dynamic journey towards digital transformation. According to Chai (2022), the Sarawak Digital Economic Strategy Book 2018–2022 was launched in 2017 by Sarawak’s Chief Minister which marks the start of the digitalization transformation in Sarawak. Sarawak’s journey towards becoming a digitally empowered state holds great promise. The Sarawak state government developed the Sarawak Digital Economy (SDE) which attempts to bring the local population in step with the global economic trend of 'going digital' (Ahmad et al., 2020). Post-pandemic, the state government introduced Post Covid-19 Development Strategy (PCDS 2030) which seeks to make Sarawak a vibrant society powered by data and innovation (Ashari & Farouk, 2023). PCDS 2030 intends to develop Sarawak into a high-income state by 2030. Jugah et al. (2022) added that Sarawak's digital transformation initiative is one of the endeavours to change the state's economy into a digital economy by 2030. Sarawak's digital transformation is a significant step toward economic modernization and inclusive development. According to Ashari and Farouk (2023), the Sarawak Digital Economy strategy calls on the government to guide and assist in a digital transformation of the industry, communities, and other stakeholders. The state of Sarawak aims to harness the benefits of technology to create opportunities for growth, innovation, and social improvement through its digital economy strategy.

To the authors' knowledge, there are several studies conducted in this field in the Sarawak context. Serojai et al. (2021) conducted a study to assess e-commerce readiness in the Sarawak context. A study on public readiness and acceptance of Sarawak's digital economy was conducted by Jugah et al. (2022). However, this is a case study in Kuching, Sarawak. The population of the study is limited to the population of Kuching Sarawak only. Subsequently, Mahdi et al. (2019) conducted a study on individual’s e-readiness indicators in Sarawak. Hence, the research gap exists due to limited studies measuring consumers' perspectives on cybersecurity readiness in Sarawak's digital transformation efforts. This study differs by addressing the underexplored aspect of Sarawak’s digital transformation by measuring the psychological factors influencing digital consumers' readiness to engage with cybersecurity measures in Sarawak’s digital transformation

2.3 Unified Theory of Acceptance and Use of Technology (UTAUT)

The Unified Theory of Acceptance and Use of Technology (UTAUT) was first introduced in 2003 by Venkatesh et al. (2003). The UTAUT is a theoretical framework for understanding and predicting people's attitudes and behaviours toward technology. Listiyani and Princes (2024) added that the UTAUT measures users' adoption of information systems. According to Aytekin et al., (2022), there are four main variables in the UTAUT model namely facilitating conditions, effort expectancy, social influence and performance expectancy. UTAUT remains important, particularly in light of rapid technology breakthroughs such as Artificial Intelligence, the Internet of Things (IoT), and Blockchain.

UTAUT was created to answer the need for a unified model of technology acceptance based on the strengths of existing theories. The UTAUT model was developed based on several theories namely the Theory of Planned Behaviour, the Diffusion of Innovation Theory, the Theory of Reasoned Action, and the Technology Acceptance Model as theoretical foundations (Boomer et al., 2022). The UTAUT model was applied to assess cybersecurity readiness within digital transformation efforts in various studies. Aflah and Taufik (2024) used UTAUT to explore behavioural acceptance and security behaviour throughout the implementation of a digital workplace. The findings revealed that the UTAUT model is a reliable predictor of behavioural acceptance of cybersecurity. A study using the UTAUT model on the role of trust and risk in citizens' adoption of e-government services was conducted by Li (2021). The study indicated that UTAUT characteristics are significant predictors for the adoption of e-government services. On top of that, Afzal et al. (2024) conducted a study on cybersecurity awareness in India using UTAUT and the study proved that UTAUT is a significant model for measuring cybersecurity awareness.

According to Xue et al. (2024), the UTAUT model has proved its broad applicability by being widely used in variety of sectors. In addition, the model has been used and proven to study the adoption of various technologies (Ayaz & Yanartas, 2020; Budhathoki et al., 2024; Mensah & Khan, 2024). Hence, the UTAUT serves as the theoretical foundation for proposing the conceptual model in this study. This study expands the UTAUT paradigm to include perceived security and awareness to create a comprehensive model capable of measuring cybersecurity readiness in Sarawak's digital transformation. Integrating UTAUT into the study provides a structured way to evaluate the readiness of Sarawak's population.

2.4 Research Hypothesis

2.4.1 Performance Expectancy (PE)

Venkatesh et al. (2003) defined performance expectancy as the level to which utilizing a technology will help customers in carrying out specified operations. In other words, performance expectancy refers to the degree to which an individual believes that using a particular technology or system will enhance their job performance or overall experience. Boomer et al. (2022) further defined performance expectancy as the degree to which people believe a technology will benefit them when engaged in a certain activity. In this study context, performance expectancy is defined as the degree to which individuals or organizations believe that using robust cybersecurity measures will enhance operational performance, efficiency, and security outcomes.

Whittaker and Noteboom (2019) in their study on the adoption of cybersecurity found that performance expectancy is significant in predicting the behavioural intention. Performance expectancy was also found to be significant in a study on behavioural acceptability and security behaviour in the introduction of digital workplaces by Aflah and Taufik (2024). A high level of performance expectancy drives a stronger commitment to cybersecurity practices. Hanif and Lallie (2021) found that performance expectancy is significant as the security factor in a study conducted in the United Kingdom. Performance expectancy plays a significant role in measuring cybersecurity readiness as it reflects the extent to which individuals believe that adopting cybersecurity measures will improve their effectiveness and enhance security outcomes in the digital environment. As a result, the authors put forward the hypothesis that:

- H1 - Performance expectancy (PE) significantly impacts the behavioural intention (BI) of digital consumers in measuring cybersecurity readiness in Sarawak’s digital transformation efforts.

2.4.2 Effort Expectancy (EE)

Venkatesh et al. (2003) defined effort expectancy as the level of ease associated with customers' use of technology. Effort expectancy refers to the extent to which an individual perceives that using a particular technology or system will be effortless and easy to navigate. According to Rizkalla et al. (2024), effort expectancy refers to how people perceive the technology's usability. In this study context, effort expectancy refers to the perceived ease or difficulty of adopting and using cybersecurity tools, protocols, and practices.

Various studies concerning cybersecurity found that effort expectancy is significant (Alraja et al., 2016; Catherine et al., 2017; Hasani et al., 2023). Effort expectancy has a big impact on measuring cybersecurity preparedness because it represents people's opinions of the ease of utilizing cybersecurity technologies and following security protocols. Therefore, understanding effort expectancy is critical for accurately measuring cybersecurity readiness and encouraging widespread adoption of secure behaviours. In light of this, the authors hypothesize that:

- H2 - Effort expectancy (EE) significantly impacts the behavioural intention (BI) of digital consumers in measuring cybersecurity readiness in Sarawak’s digital transformation efforts.

2.4.3 Social Influence (SI)

Social influence is the extent to which customers assume that prominent people believe they should utilize a given technology (Venkatesh et al., 2003). Lim (2022) refers to social influence as how society impacts a person to shape their beliefs, perceptions, values, attitudes, intentions, and behaviours. In the context of measuring cybersecurity readiness, social influence refers to the extent to which individuals perceive those significant others believe they should adopt and adhere to cybersecurity practices.

Li (2021) in a study found that social influence is a significant factor in determining the e-government services adoption. Aflah and Taufik (2024) further proved the significance of social influence in a study on behavioural acceptance and security behaviour. Measuring cybersecurity readiness should consider social influence factors to assess how effectively a security-oriented culture supports readiness efforts. As a result, the authors propose the following hypothesis:

- H3 - Social influence (SI) significantly impacts the behavioural intention (BI) of digital consumers in measuring cybersecurity readiness in Sarawak’s digital transformation efforts.

2.4.4 Facilitating Conditions (FC)

Facilitating conditions refer to consumers' assessment of the resources and support available to undertake a behaviour (Venkatesh et al. 2003). Facilitating Conditions encompass the resources, infrastructure, and external factors that enable an individual to effectively use a technology or system. According to Buraimoh et al. (2023), facilitating conditions are the availability of resources to promote mobile technology uptake and use. In this study context, facilitating conditions are the resources, infrastructure, and organizational environment that allow individuals and organizations to successfully adopt and implement cybersecurity measures.

Mansour et al. (2021) in their study found that facilitating conditions are significant in determining the adoption of e-government services among SMEs in Saudi Arabia. Besides, Salimon et al. (2018), also found that facilitating conditions as a significant factor in a study on trust among e-banking customers in Nigeria. Li (2021), in a study on e-government adoption, found that facilitating conditions as a significant variable. Consequently, the authors suggest the following hypotheses:

- H4 - Facilitating conditions (FC) significantly impact the behavioural intention (BI) of digital consumers in measuring cybersecurity readiness in Sarawak's digital transformation efforts.
- H5 - Facilitating conditions (FC) significantly impact cybersecurity readiness (CR) in Sarawak's digital transformation efforts.

2.4.5 Perceived Risk (PR)

Perceived risk refers to negative consumer perception of utilizing services that relate to losses (Zadha & Suparna, 2023). In simpler definition, perceived risk is a psychological concept that influences how people assess the possible dangers or drawbacks of a situation before taking action. Rajendran and Jayakrishnan (2018) defined perceived risk as the perception of a particular product or service that yields unexpected outcomes. Perceived risk is the amount to which undesirable effects of an economic event may occur which affects individuals, enterprises, organizations, or governments (Bland et al., 2024). In this study context, perceived risk refers to an individual's subjective judgment about the potential negative outcomes or uncertainties associated with engaging in a particular digital product or service.

Abdelhamid et al. (2019) in their study found that perceived risk is a significant factor in determining e-services avoidance among American adults. Perceived risk as a cybersecurity factor was further proven as a significant factor in e-government execution in Saudi Arabia (Al-Zahrani, 2020). Besides, Hilowle et al. (2022) also found that perceived risk as a significant factor in the adoption of national digital identity systems in Australia. Perceived risk has a substantial impact on measuring cybersecurity readiness because it influences how individuals and organizations perceive the importance and urgency of implementing security measures. Thus, the authors hypothesize the following:

- H6 - Perceived risk (PR) significantly impacts the behavioural intention (BI) of digital consumers in measuring cybersecurity readiness in Sarawak's digital transformation efforts.
- H7 - Perceived risk (PR) significantly impacts cybersecurity readiness (CR) in Sarawak's digital transformation efforts.

2.4.6 Cybersecurity Awareness (CA)

According to Al-Fatlawi (2024), cybersecurity awareness comprises teaching individuals the importance of protecting customer data privacy, people's identities, and other assets that are exposed to hackers. Cybersecurity awareness involves understanding and using safeguards against online threats and vulnerabilities (Abdullah et al., 2023). Cybersecurity awareness refers to the knowledge, understanding, and attitude that individuals or organizations have regarding protecting their information systems, data, and digital assets from cyber threats.

According to Hasani et al. (2023), cybersecurity awareness is an important consideration in investigating privacy-enhancing technology adoption. Besides, Afzal et al. (2024), found that cybersecurity awareness is significant in determining the payment banking adoption in India. On top of that, Benjamin et al. (2024) proved that awareness is essential in studying the digital transformation in Small and Medium Enterprises (SMEs). Effective cybersecurity readiness evaluation must consider users' degree of cybersecurity awareness to ensure that they are ready to actively participate in a safe digital environment. Consequently, the authors propose the following hypotheses:

- H8 - Cybersecurity awareness (CA) significantly impacts the behavioural intention (BI) of digital consumers in measuring cybersecurity readiness in Sarawak's digital transformation efforts.
- H9 - Cybersecurity awareness (CA) significantly impacts cybersecurity readiness (CR) in Sarawak's digital transformation efforts.

2.4.7 Behavioral Intention (BI)

Behavioural intention refers to people's subjective capacity or willingness to interact and perform in a given way (Hasbie et al., 2023). Behavioural intention is often seen as a precursor to actual behaviour. According to Putra et al. (2019), behavioural intention is a consumer's purposeful decision to do something. Behavioural intention in the context of cybersecurity readiness refers to the willingness or intention of individuals or organizational members to engage in cybersecurity practices and measures.

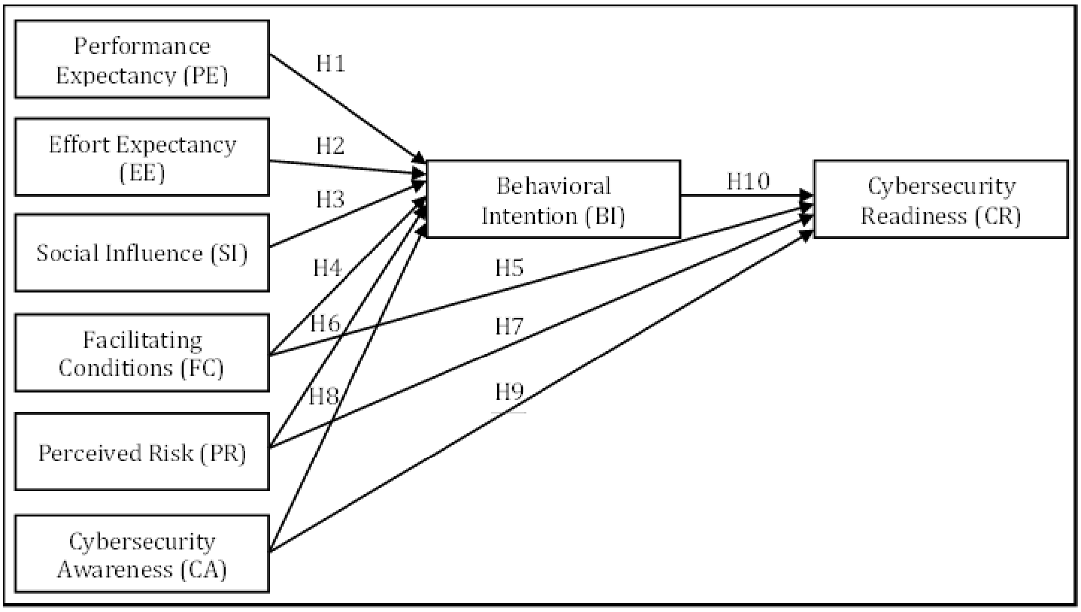
Sivarethinamohan and Sujatha (2021) in their study proved the significance of behavioural intention in predicting the actual use of cyber defences in the Asia-Pacific region. Jamil et al. (2024) found that behavioural intention is important in computer security usage. Besides, Hasani et al. (2023) noted that behavioural intention is significant in the adoption of cybersecurity. Behavioural intention plays a fundamental role in shaping the level of cybersecurity readiness. Thus, the authors propose the following hypothesis:

- H10 - Behavioural intention significantly impacts the cybersecurity readiness in Sarawak's digital transformation efforts.

2.5 Conceptual Framework

Figure 1 depicts the conceptual framework of the study. The conceptual framework was adapted and developed based on UTAUT. According to Lahcen et al. (2020), research should expand into understudied areas such as behavioural aspects of cybersecurity, as most cyber incidents are due to human error. Perceived risks and cybersecurity awareness are integrated into the conceptual framework to give a holistic understanding of evaluating cybersecurity readiness in Sarawak's digital transformation efforts.

According to Zahiroh (2020), cybersecurity awareness is essential to face changes toward digitization and technological advances. Awareness of cybersecurity empowers consumers with the knowledge to mitigate cyber threats. Additionally, perceived risk is one of the main barriers to the adoption or acceptance of new advanced technology (Almaiah et al., 2023). Perceived risk reflects concerns about potential threats that hinder digital transformation and adoption. Hence, incorporating these two variables into the research model for evaluating cybersecurity readiness within Sarawak's digital transformation efforts is vital due to their significant and unique contributions.


Performance Expectancy (PE)
Effort Expectancy (EE)
Social Influence (SI)
Facilitating Conditions (FC)
Perceived Risk (PR)
Cybersecurity Awareness (CA)
Behavioral Intention (BI)
Cybersecurity Readiness (CR)
H1
H2
H3
H4
H5
H6
H7
H8
H9
H10

(a)

Fig. 1 *(a) The study's conceptual framework (Source: Adapted from Ayaz and Yanartas, 2020)*

3. Methodology

This study adopted a quantitative research approach with the primary aim of assessing the psychological factors influencing digital consumers' readiness to engage with cybersecurity measures in Sarawak's digital transformation. The quantitative research technique enables data collection from a large sample (Ghanad, 2023).

Additionally, the study utilized a cross-sectional survey design. According to Wang and Cheng (2020), cross-sectional studies examine data from a population at a certain point in time. The cross-sectional survey design enabled data collection from a diverse set of Sarawak consumers at a specific point in time.

The research location was in Sarawak, Malaysia. Sarawak, which is a state within Malaysia is well-known for its diverse religion, culture, and tradition (Sageng et al., 2020). Sarawak is divided into 11 divisions and 31 districts with around 40 sub-ethnic groups (Ahmad et al., 2020). According to Tang et al. (2022), Sarawak has been making substantial efforts towards digital transformation. Therefore, Sarawak provided an ideal setting to explore consumers' perspectives on cybersecurity readiness in the context of digital transformation. The target population for this study was digital consumers in Sarawak. According to Szwajca (2019), a digital consumer refers to a buyer who uses their mobile device to interact with market sellers of products and services. In this study context, digital consumers refer to individuals engaged in various online activities, including e-commerce, online banking, social media, digital entertainment, and the use of government services. This broad group encompassed diverse age groups, educational backgrounds, professions, and geographic locations within Sarawak.

The sample size was determined via Krejcie and Morgan's (1970) published table on sample size. The total population of Sarawak was 2,907,500 based on the population census 2020 which was conducted every 10 years (The official portal of Sarawak Government, 2024). Hence, the minimum sample size for this study was set at 384 based on the Krejcie and Morgan (1970) sample size table. Additionally, the sampling method for this study was purposive random sampling. Purposive random sampling is a non-probability sampling technique in which the sample is chosen exclusively on the basis of the researcher's knowledge and judgment (Ebenezer & Piate, 2023). This strategy involved purposefully selecting individuals who met specific pre-defined criteria related to the research objectives. According to Friday and Leah (2024), purposive sampling was employed in most studies to ensure a high-quality sample free of biases. The selection criteria required participants to be digital consumers residing in Sarawak who frequently use digital services and have experience or engagement with basic cybersecurity practices.

The research tool for this study was a questionnaire designed to collect complete data from potential respondents. The questionnaire consisted of Section A about the demographic information of respondents and Section B utilised a 5-point Likert scale to gather information pertaining to the main objective of the study. The questionnaires were distributed through self-administration and online platforms, including email, social media, and Google Forms. According to Dalati and Gomez (2018), the advantages of self-administered questionnaires included minimal cost, reduced bias error and increased anonymity. The questionnaire items were developed based on an extensive review of existing literature within the same niche area of cybersecurity readiness (refer to Appendix section). The questionnaire was designed to measure each of the independent variables and their relationship to consumers' behavioural intention and cybersecurity readiness. The data collection process spans over a period of 7 months (from April 2024 to December 2024).

The study's data analysis was performed using SmartPLS 4.0 software. SmartPLS software was based on a modern Java-based programming environment that allowed for a graphical user interface for PLS-SEM (Memon et al., 2021). The software was an effective tool for performing Partial Least Squares Structural Equation Modeling (PLS-SEM). According to Dash and Paul (2021), the PLS-SEM technique is an ideal method for predicting and testing theory development. There were two stages of data analysis in the PLS-SEM, namely measurement model assessment and structural model assessment. According to Al-Marsomi and Al-Zwainy (2023), it is critical to examine the measurement's validity and reliability before creating study results when developing PLS-SEM. This step ensured that the indicators reliably measured their corresponding latent constructs. The structural model was then evaluated after confirming the measurement model. According to Hair et al. (2021), the aim of structural model assessment in PLS-SEM is to examine the model's explanatory and predictive capabilities. The structural model examined the hypothesized relationships between the latent variables.

4. Data Analysis

4.1 Preliminary Data Analysis

It is necessary to perform data cleaning, coding, and entry before the actual data analysis process. The first task in this preliminary data analysis stage was to check for any missing data and outlier detection. According to Arundel (2023), data cleansing is critical to guaranteeing the validity and reliability of survey results. The next step is outlier detection. According to Uher et al. (2022), the outlier detection process identifies observations that appear to be incongruous with the remainder of the dataset. Any extreme values will be identified and removed as outliers can distort the model's estimation. A total of 455 questionnaires were distributed to potential respondents, with 55 discarded due to incomplete responses, missing data, and outlier detection. As a result, 400 usable questionnaires were retained for data analysis.

Additionally, the issue of Common Method Bias (CMB) was then examined. According to Kock et al. (2021), CMB can have a negative impact on a study's validity. Kock (2015) added that the identification of CMB is generated through a full collinearity test based on Variance Inflation Factors (VIF). Table 1 below shows the VIF value of the study which ranged from 1.161 to 1.804. VIF values above 5 or 10 indicate problematic collinearity (Belsley, 1991). Hence, it is safe to say that the study was free from CMB.

Table 1 *VIF value of the study*

	VIF
BI -> CR	1.161
CA -> BI	1.192
CA -> CR	1.170
EE -> BI	1.181
FC -> BI	1.493
FC -> CR	1.454
PE -> BI	1.245
PR -> BI	1.804
PR -> CR	1.526
SI -> BI	1.665

Note *Performance expectancy (PE); effort expectancy (EE); social influence (SI); facilitating conditions (FC); perceived risk (PR); cybersecurity awareness (CA); behavioral intention (BI); cybersecurity readiness (CR)*

4.2 Demographic Profile of Respondents

Table 2 *Demographic information of respondents*

	Total	Percent (%)
Gender		
Male	196	51.04
Female	188	48.96
Age Group		
Under 18	68	17.71
18-34	98	25.52
35-49	105	27.34
50-64	103	26.82
65 and above	10	2.60
Education Level		
No formal education/ Primary school	23	5.99
Secondary school	68	17.71
Post-secondary school (Diploma, Certificate & etc.)	163	42.45
Bachelor degree or higher	130	33.85
Ethnicity		
Malay	115	29.95
Chinese	122	31.77
Indigenous (Iban, Bidayuh, Orang Ulu & etc.)	127	33.07
Others	20	5.21
Geographic Location		
West Sarawak (Kuching, Bau, Lundu & Serian)	105	27.34
East Sarawak (Miri, Bintulu, Marudi & Baram)	90	23.44
Coastal Sarawak (Sibu, Sarikei, Mukah & Bintulu)	110	28.65
Interior Sarawak (Kapit, Limbang, Belaga, Song & Ulu Baram)	79	20.57

Table 2 shows the demographic information of the respondents in the study. The number of Male respondents (51.04%) was slightly higher than the number of female respondents (48.96%). In terms of age group, the age group of 35-49 (27.34%) represents the highest number followed by 50-64 (26.82%), 18-34 (25.52%), and under 18 (17.71%) respectively. The age group of 65 and above (2.60%) represents the lowest number of respondents in the study.

In terms of education level, the education level of post-secondary school (Diploma, Certificate and etc.) represents the highest number of respondents at 42.45%. Subsequently, the education level of bachelor degree or higher (33.85%) and secondary school (17.71%) come second and third highest. Education level of no formal education/ primary school represents the lowest number of respondents at 5.99%.

The ethnicity of indigenous (Iban, Bidayuh, Orang ulu & etc.) represents the highest number of respondents at 33.07%. Ethnicities of Chinese and Malay represent the second and third highest number of respondents at 31.77% and 29.95% respectively. Others represent the lowest number at 5.21%.

Lastly, the geographical location of Coastal Sarawak represents the highest number of respondents at 28.65%. The geographical location of West Sarawak and East Sarawak come at the second and third highest number of respondents at 27.34% and 23.44% respectively. The geographical location of Interior Sarawak represents the lowest number of respondents at 20.57%.

4.3 Measurement Model Assessment

The measurement model assessment refers to the process of evaluating how well the manifest variables represent the underlying latent variables (Henseler et al., 2015). This study employed a reflective model. The key criteria of the reflective measurement model assessment are indicator reliability, internal consistency reliability, convergent validity, and discriminant validity (Hair et al., 2021). Based on Table 3 below, the outer loading values of the study ranged from 0.807 to 0.969. According to Hair et al. (2017), the outer loading values should be higher than 0.708 to determine indicator reliability. Table 3 shows the Outer Loadings values of the Study. Hence, the indicator reliability of the study was ensured.

Subsequently, the internal consistency reliability of the study was determined via Cronbach's Alpha and Composite Reliability (CR). To establish internal consistency reliability, the value of Cronbach's Alpha and CR must be higher than 0.7 (Ali et al., 2018). Based on Table 4 below, the values of Cronbach's Alpha and CR (rho a and rho c) were higher than the minimum threshold of 0.7. Hence, the internal consistency reliability of the study was established. Table 4 represents the reliability and AVE results of the study.

Average Variance Extracted (AVE) was used to establish the convergence validity of the study. The AVE value of the study ranged from 0.732 to 0.894 which exceeded the recommended threshold of 0.5 and above by Hair et al. (2017) (see Table 4). Hence, the convergent validity of the study was established. On top of that, the discriminant validity of the study was tested using the Heterotrait-Monotrait ratio (HTMT) and Fornell-Larcker Criterion tests. The HTMT value of the study is below the maximum threshold of 0.85 as recommended by Henseler et al. (2015) (see Table 5). Table 5 shows the HTMT test result of the study. Next, the square root of AVE in each latent variable should be greater than other correlation values among the latent variables to establish discriminant validity in the Fornell-Larcker Criterion test. Table 6 shows the Fornell-Larcker Criterion result of the study. The discriminant validity of the study was established since all the criteria were met.

Table 3 *Outer loadings of the study*

	Outer loadings
BI1 <- BI	0.953
BI2 <- BI	0.912
BI3 <- BI	0.964
CA1 <- CA	0.867
CA2 <- CA	0.842
CA3 <- CA	0.864
CA4 <- CA	0.847
CR1 <- CR	0.960
CR2 <- CR	0.875
CR3 <- CR	0.965
EE1 <- EE	0.935
EE2 <- EE	0.931
EE3 <- EE	0.812
FC1 <- FC	0.935

	Outer loadings
FC2 <- FC	0.923
FC3 <- FC	0.950
PE2 <- PE	0.807
PE3 <- PE	0.969
PR1 <- PR	0.957
PR2 <- PR	0.934
PR3 <- PR	0.945
SI1 <- SI	0.915
SI2 <- SI	0.918
SI3 <- SI	0.945
PE1 <- PE	0.953

Table 4 *Reliability and AVE results of the study*

	Cronbach's alpha	Composite reliability (rho_a)	Composite reliability (rho_c)	Average variance extracted (AVE)
BI	0.938	0.942	0.960	0.890
CA	0.878	0.878	0.916	0.732
CR	0.926	0.937	0.954	0.873
EE	0.880	0.952	0.923	0.800
FC	0.929	0.930	0.955	0.876
PE	0.931	0.767	0.937	0.833
PR	0.940	0.942	0.962	0.894
SI	0.918	0.951	0.948	0.858

Table 5 *HTMT test result of the study*

	BI	CA	CR	EE	FC	PE	PR	SI
BI								
CA	0.332							
CR	0.264	0.489						
EE	0.072	0.206	0.070					
FC	0.035	0.188	0.164	0.101				
PE	0.036	0.354	0.354	0.428	0.173			
PR	0.143	0.204	0.138	0.098	0.587	0.073		
SI	0.051	0.335	0.266	0.195	0.478	0.184	0.626	

Table 6 *Fornell-Larcker criterion result of the study*

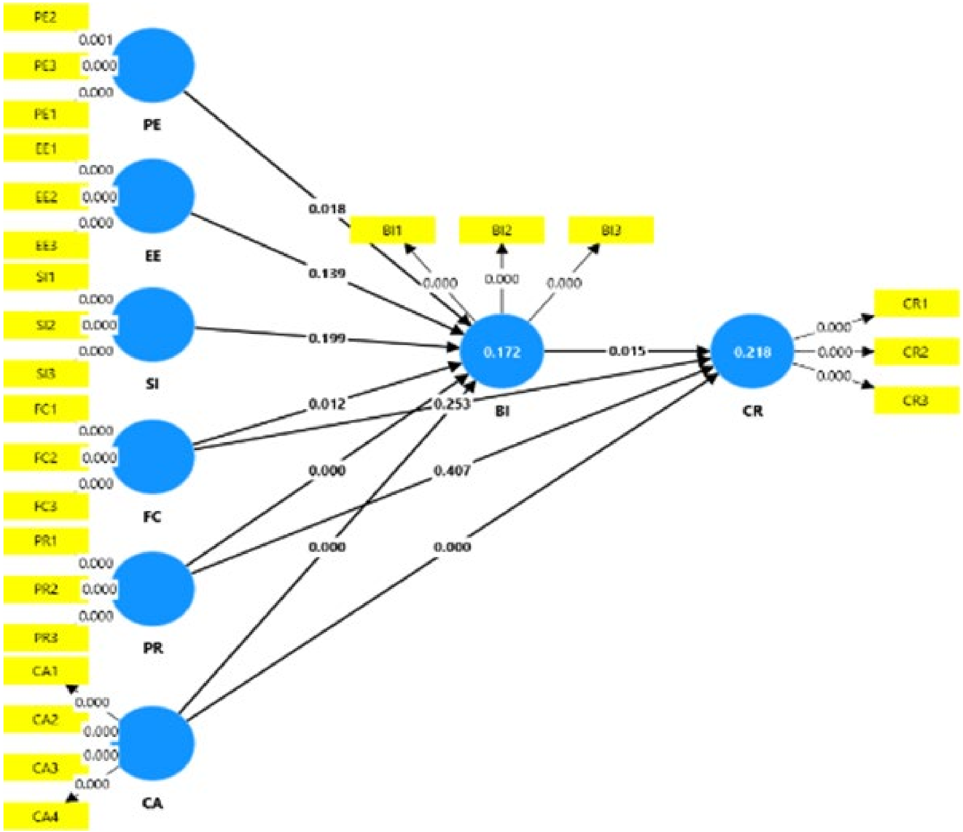
	BI	CA	CR	EE	FC	PE	PR	SI
BI	0.943							
CA	0.302	0.855						
CR	0.246	0.444	0.934					
EE	0.069	0.187	0.071	0.894				
FC	0.032	0.171	0.152	0.096	0.936			
PE	0.043	-0.298	-0.286	-0.364	-0.142	0.913		
PR	0.136	-0.186	-0.130	-0.094	-0.547	0.058	0.945	
SI	-0.049	0.301	0.240	0.182	0.437	-0.129	-0.580	0.926

4.4 Structural Model Assessment

The next step in the data analysis was the assessment of the structural model, following the establishment of the measurement model. Bootstrapping with 5000 resamples was employed in the structural model assessment to test the hypotheses of the study. Figure 2 below shows the result of the path coefficient in a graphical presentation.

The R2 and Q2 were utilised to assess the structural model of the study. R2 measures a model's prediction accuracy (Zeng et al., 2021). The study established the predictive accuracy as the R2 values of the study exceeded the minimum threshold of 0.1 recommended by (Falk & Miller, 1992) (see Table 7). Next, Q2 is essential for determining the predictive relevance of a structural model (Hair et al., 2014). Acceptable Q2 values are 0.02 (weak), 0.15 (moderate), and 0.35 (sound) (Chin, 2010). The structural model of this study had predictive relevance because all the Q2 values were above 0 (see Table 7). Table 7 shows the result of path coefficient, hypothesis testing, Q2 and R2. On top of that, Standardized Root Mean Square Residual (SRMR) was used to further assess the model fit. According to Goretzko et al., (2024), one of the most common measures of model fit is the SRMR. The SRMR value of 0.08 is deemed acceptable by Hu and Bentler (1999). The study portrays an acceptable model fit with SRMR values of 0.041 and 0.052 (see Table 8). Table 8 represents the result of SRMR test.

Further assessment of goodness of fit, all ten hypotheses were tested to achieve the main objective of the study. Based on the bootstrapping result, six out of ten hypotheses of the study were supported. The result showed that PE (β = 0.187, τ = 2.370, p < 0.05), FC (β = 0.152, τ = 2.503, p < 0.05), PR (β = 0.238, τ = 4.029, p < 0.05) and CA (β = 0.385, τ = 7.561, p < 0.05) were found to be supported in determining the behavioural intention of digital consumers in cybersecurity readiness in Sarawak's digital transformation efforts. Contrarily, EE (β = 0.089, τ = 1.481, p > 0.05) and SI (β = -0.085, τ = 1.284, p > 0.05) were found to be not significant in determining behavioural intention. Additionally, BI (β = 0.134, τ = 2.439, p < 0.05) and CA (β = 0.385, τ = 7.191, p < 0.05) were found to be supported in determining the cybersecurity readiness among consumers in Sarawak's digital transformation efforts. Contrarily, FC (β = 0.058, τ = 1.144, p > 0.05) and PR (β = -0.045, τ = 0.829, p > 0.05) were found to be not significant in determining cybersecurity readiness.



(a)

Fig. 2 *(a) Graphical output of path coefficient*

Table 7 *Result of path coefficient, hypothesis testing, Q^2 and R^2*

		β	T statistics	P values	Decision
H1	PE -> BI	0.187	2.370	0.018	Supported
H2	EE -> BI	0.089	1.481	0.139	Not Supported
H3	SI -> BI	-0.085	1.284	0.199	Not Supported
H4	FC -> BI	0.152	2.503	0.012	Supported
H5	FC -> CR	0.058	1.144	0.253	Not Supported
H6	PR -> BI	0.238	4.029	0.000	Supported
H7	PR -> CR	-0.045	0.829	0.407	Not Supported
H8	CA -> BI	0.385	7.561	0.000	Supported
H9	CA -> CR	0.385	7.191	0.000	Supported
H10	BI -> CR	0.134	2.439	0.015	Supported
	R^2	Q^2			
BI	0.172	0.130			
CR	0.218	0.179			

Table 8 *Result of SRMR test*

	Original sample (O)	Sample mean (M)	95%	99%
Saturated model	0.041	0.040	0.109	0.145
Estimated model	0.052	0.042	0.108	0.145

4.5 Discussion

The study aims to shed light on the psychological factors influencing digital consumers' readiness to engage with cybersecurity measures in Sarawak's digital transformation. As expected, the study reveals that performance expectancy is significant in determining the behavioural intention of digital consumers toward cybersecurity readiness. This finding is in accordance with other studies' findings (Ain et al., 2015; Engotoit et al., 2016; Muller & Lind, 2020). The active efforts of the government and organizations to enhance cybersecurity readiness contribute to consumers' confidence in using digital services. Effective regulations have been implemented to ensure Sarawak maintains a secure and cyber-resilient environment (Sarawak Multimedia Authority, 2023). This builds consumers' confidence and influences their behavioural intentions toward engaging with Sarawak's digital transformation initiatives.

Surprisingly, the study found that effort expectancy is not significant in determining the behavioural intention of digital consumers toward cybersecurity readiness. This finding concurs with the findings of other studies (Etim & Daramola, 2023; Marsintauli et al., 2023; Muller and Lind, 2020). The finding of this study indicates that effort expectancy does not contribute to cybersecurity readiness among digital consumers. The state government created a specialized Cyber Security Unit to offer cybersecurity services and support to the government, businesses, and citizens in the state (CyberSarawak, 2024). This initiative has increased consumers' confidence in the effectiveness and accessibility of cybersecurity services in the state. This initiative improves the availability, effectiveness, and accessibility of cybersecurity services. As a result, it becomes easier for consumers to protect themselves from digital threats. This leads to the insignificance of effort expectancy in shaping consumers' behavioural intentions.

In addition, the study reveals that social influence is not significant in determining the behavioural intention of digital consumers toward cybersecurity readiness. This finding of the study is in line with the finding by Muller and Lind (2020). As cybersecurity becomes a widely understood necessity, consumers may prioritize their own personal awareness and concerns over cybersecurity over the influence of others. The emphasis on regulatory frameworks and government-led cybersecurity initiatives leads consumers to trust the systems in place. This makes digital consumers become less reliant on external social influences. Contrarily, other studies (Alqahtani & Erfani, 2021; Etim & Daramola, 2023) found that social influence was significant in determining cybersecurity compliance in different contexts and regions. This suggests that the impact of social influence on individuals' cybersecurity behaviours can vary depending on local factors such as cultural norms, societal expectations, or community-based practices. Besides, different regions and contexts may have different scenarios that affect the prominence of social influence in determining cybersecurity readiness.

The study reveals that facilitating conditions have a significant impact on the behavioural intention of digital consumers toward cybersecurity readiness. This finding is in tandem with the findings of other studies (Alqahtani & Erfani, 2021; Hasan et al., 2021) in the same field. Facilitating conditions, such as access to the necessary tools, infrastructure, and support systems, ensure that consumers are able to engage with cybersecurity measures easily. These facilitating conditions help reduce barriers to encourage consumers to act on their intention to maintain a secure digital environment. Surprisingly, facilitating conditions do not contribute to cybersecurity readiness. This finding is consistent with Etim and Daramola (2023), who reported similar results. Despite improvements in digital infrastructure, there are still significant barriers that may hinder consumers from effectively engaging with cybersecurity measures. One major challenge in Sarawak is the digital divide between urban and rural areas (Sulaiman & Halamy, 2021). Urban centres may have relatively better access to high-speed internet and modern devices. In contrast, rural areas, particularly remote villages, often struggle with limited or unreliable internet connectivity. Additionally, these areas face challenges due to a lack of access to updated technologies. This creates a disparity in the availability of resources, making it difficult for people in rural areas to engage with cybersecurity measures effectively.

The finding of this study reveals that perceived risk is proven to be an essential variable in determining the behavioural intention of consumers towards cybersecurity readiness. This revelation concurs with other studies (AlMeraj et al., 2023; Bharathi, 2019; Creazza et al., 2022). Digital consumers in Sarawak who perceive a high level of risk regarding their personal data or online activities are more likely to engage in behaviours that enhance their cybersecurity readiness. However, perceived risk does not contribute to their cybersecurity readiness. This finding is supported by other studies (Al-Emran et al., 2024; Rattanapong & Ayuthaya, 2025). Even though consumers may perceive risks, they might underestimate the actual likelihood or severity of these risks happening to them personally. This can lead to a lower sense of urgency to engage in cybersecurity practices. They may not fully believe that they are at risk or that the consequences of a breach would be severe enough to warrant action.

Cybersecurity awareness is found to be an essential variable in determining behavioural intention and cybersecurity readiness among digital consumers in Sarawak. This finding aligns with previous studies by Chapman and Reithel (2021) and Falowo et al. (2022). Additionally, Liu et al. (2020) performed a qualitative study on the perceptions about cybersecurity and found that awareness is an essential variable. Digital consumers with greater cybersecurity awareness are better equipped to make informed decisions about their digital safety. This leads to stronger behavioural intentions to adopt security measures such as using strong passwords, enabling two-factor authentication, and avoiding risky online behaviour. Cybersecurity awareness empowers consumers to recognize the importance of protecting their personal information such as financial data, login credentials, and other sensitive data.

Finally, behavioural intention is significant in determining cybersecurity readiness among digital consumers in Sarawak. This finding concurs with other studies (Avina et al., 2017; Choi et al., 2018; and Safa et al., 2016). As digital consumers become more aware of the increasing risks of cyber threats, their intention to engage with cybersecurity measures grows. This awareness often translates into a stronger intention to protect personal data, secure online transactions, and engage with cybersecurity practices. Consumers are more likely to take actions that ensure their security online with the growing use of digital platforms and services.

5. Conclusion

Theoretically, the study adapts and extends the UTAUT by applying its constructs to the specific field of cybersecurity readiness. UTAUT traditionally focuses on technology adoption, but this research broadens its application by incorporating cybersecurity-related behaviours. By introducing new variables such as cybersecurity awareness and perceived risk, the study offers an enriched version of UTAUT that can better explain digital consumers' intentions and behaviours in the context of cybersecurity. Expanding UTAUT allows for a more accurate representation of how people adopt security measures and make decisions regarding cybersecurity in today's digital environment. As Sarawak undergoes significant digital transformation, understanding cybersecurity readiness helps ensure that the population is prepared to address potential risks and challenges associated with these technological changes.

Subsequently, the findings of the study offer important implications for policymakers in Sarawak. Based on the findings, the study suggests that future policies should focus on improving public awareness about cybersecurity and offering easy access to resources. Additionally, it recommends addressing risk concerns. This can lead to better-targeted government initiatives and regulations to promote cybersecurity readiness across digital consumers. The study's findings help bridge the gap between cybersecurity policies and actual consumer behaviour. By understanding which factors contribute to cybersecurity readiness, efforts can be made to reduce the cybersecurity preparedness gap in Sarawak. This ensures that consumers are not only aware of the risks but are also motivated and equipped to protect themselves in the digital environment.

It is crucial for businesses and organizations in Sarawak to fully understand consumer behaviour related to cybersecurity readiness. Businesses can tailor their products and services to meet the specific needs and concerns of digital consumers to improve adoption rates. For instance, a digital learning platform may focus on cybersecurity education features to build awareness and trust with users. Personalized security features or easy-to-understand security guidelines could help consumers feel more secure and encourage greater usage of the platform or service.

While this study offers valuable insights into the psychological factors influencing cybersecurity readiness among digital consumers in Sarawak, several limitations should be acknowledged. First, the findings are limited to a single geographic region, which may restrict the generalizability of the results to other parts of Malaysia or different global contexts. Regional variations in digital infrastructure, cultural attitudes, and cybersecurity awareness could influence consumer behaviour differently. Therefore, future studies are encouraged to apply and test the proposed conceptual model across other regions or countries to uncover context-specific patterns and develop more targeted cybersecurity strategies.

Second, this study employed a cross-sectional design, capturing consumer perceptions and behaviours at a single point in time. As perceptions of cybersecurity risk and digital behaviours can evolve in response to emerging threats and technological advancements, a longitudinal approach in future research would provide deeper insights into how these factors change over time. Tracking shifts in cybersecurity readiness as digital transformation progresses would be valuable for informing dynamic policies and interventions that are responsive to consumers' evolving needs and the changing digital landscape.

Acknowledgement

We would like to thank all those who contributed to this research, including the participants and those who provided support and feedback. Their help was essential in completing this study. This research was conducted without any financial support or external funding.

Conflict of Interest

The authors declare that they have no conflicts of interest related to the publication of this paper.

Author Contribution

The contributions of each author to this research are as follows: Maximus Balla Tang and Jessica Lyn Andam were involved in the ***conceptualization and design of the study. Data collection*** *was conducted collaboratively by Maximus Balla Tang, Jessica Lyn Andam, and Mohd Ngah Ismail Suzali. All three authors contributed to the* ***analysis and interpretation of the data****. The initial* ***manuscript draft*** *was prepared by Maximus Balla Tang and Jessica Lyn Andam. All authors reviewed the manuscript critically and approved the final version for submission.*

Appendix A: Construct Section of Questionnaire

Variable	Items	Adapted from
PE	1. I find cybersecurity technologies beneficial to me.	Alhalafi and Veeraraghavan (2023)
	2. I can complete tasks faster when I use cybersecurity technologies.	
	3. Protecting my private information online is made simpler by using cybersecurity tools.	
EE	4. I find cybersecurity technologies straightforward and simple to utilize.	Alhalafi and Veeraraghavan (2023)
	5. I have the necessary skills to employ cybersecurity technology.	
	6. I find it easy to learn and use new cyber technology.	
SI	7. Those who have an impact on my actions advise me to adopt cybersecurity tools.	Alhalafi and Veeraraghavan (2023), and Camilleri (2024)
	8. I have received assistance from my co-workers in using cybersecurity technologies.	
	9. People who are important to me think that I should use cybersecurity technologies.	
FC	10. There are enough IT agencies and experts to manage cyber security.	Berlilana et al. (2021)
	11. There is enough cybersecurity infrastructure.	

	12. I have adequate technological resources for cyber security.	
PR	13. I am concerned about the potential public disclosure of confidential information.	Berlilana et al. (2021)
	14. I am concerned about the security of online activity.	
	15. I am concerned about the confidentiality of the information I send to external sources.	
CA	16. I understand the advantages of using strong cybersecurity solutions.	Mensah and Khan (2024), and Rehman et al. (2012)
	17. I have attended cybersecurity awareness training.	
	18. I am knowledgeable about cybersecurity services.	
	19. I understand the capabilities of cybersecurity technologies.	
BI	20. I plan to continue employing cybersecurity in the near future.	Alhalafi and Veeraraghavan (2023), and Berlilana et al. (2021)
	21. I will continue to utilize cybersecurity regularly.	
	22. I am excited to use cutting-edge cybersecurity technology.	
CR	23. I am committed to keeping system vulnerabilities under acceptable risks.	Hasan et al. (2021)
	24. I am devoted to proactively managing emerging threats.	
	25. I am prepared to use cybersecurity technologies to protect myself from cyber dangers.	

References

Abdelhamid, M., Kisekka, V., & Samonas, S. (2019). Mitigating e-services avoidance: The role of government cybersecurity preparedness. Information and Computer Security, 27(1), 26-46. https://doi.org/10.1108/ICS-02-2018-0024

Abdullah, Z., Dahlan, N., Dahlan, A., & Arifin, A. F. (2023). Cybersecurity awareness on personal data protection using game-based learning. Information Management and Business Review, 15(3), 497-503. https://doi.org/10.22610/imbr.v15i3(I).3559

Aflah, M. F., & Taufik, T. A. (2024). Analysis of behavioral acceptance and security behavior on implementation of digital workplace. Asian Journal of Research in Business and Management, 6(1), 37-50. https://doi.org/10.55057/ajrbm.2024.6.1.4

Afzal, M., Meraj, M., Kaur, M., & Ansari, M. S. (2024). How does cybersecurity awareness help in achieving digital financial inclusion in rural India under escalating cyber fraud scenario? Journal of Cyber Security Technology, advance online publication. https://doi.org/10.1080/23742917.2024.2347674

Ahmad, D. A., Ahmad, J., & Saad, S. (2020). Sarawak digital economy and the organisational sensemaking process of CSR: A conceptual view. Jurnal Komunikasi: Malaysian Journal of Communication, 36(1), 205-223. https://doi.org/10.17576/JKMJC-2020-3601-12

Ain, N., Kaur, K., & Waheed, M. (2016). The influence of learning value on learning management system use. Information Development, 32(5), 1306–1321. https://doi.org/10.1177/0266666915597546

Al-Emran, M., Al-Sharafi, M. A., Foroughi, B., Iranmanesh, M., Alsharida, R. A., Al-Qaysi, N., & Ali, N. (2024). Evaluating the barriers affecting cybersecurity behavior in the Metaverse using PLS-SEM and fuzzy sets (fsQCA). Computers in Human Behavior, 159, 108315. https://doi.org/10.1016/j.chb.2024.108315

Al-Fatlawi, H. H. (2024). Awareness of cyber security aspects in distance education. Journal of Pedagogical Sociology and Psychology, 6(1), 77-88. https://doi.org/10.33902/jpsp.202424403

Alhalafi, N., & Veeraraghavan, P. (2023). Exploring the challenges and issues in adopting cybersecurity in Saudi smart cities: Conceptualization of the cybersecurity-based UTAUT model. Smart Cities, 6(3), 1523-1544. https://doi.org/10.3390/smartcities6030072

Ali, F., Rasoolimanesh, S. M., Sarstedt, M., Ringle, C. M., & Ryu, K. (2018). An assessment of the use of partial least squares structural equation modeling (PLS-SEM) in hospitality research. International Journal of

Contemporary Hospitality Management, 30(1), 514-538. https://doi.org/10.1108/IJCHM-10-2016-0568

Alkharusi, H. (2022). A descriptive analysis and interpretation of data from likert scales in educational and psychological research. Indian Journal of Psychology and Education, 12(2), 13-16.

Almaiah, M. A., Al-Otaibi, S., Shishakly, R., Hassan, L., Lutfi, A., Alrawad, M., Qatawneh, M., & Alghanam, O. A. (2023). Investigating the role of perceived risk, perceived security and perceived trust on smart m-banking application using SEM. Sustainability, 15(13), 9908. https://doi.org/10.3390/su15139908

Al-Marsomi, M. S. K., & Al-Zwainy, F. M. S. (2023). Structural equation modeling of critical success factors in the programs of development regional. Journal of Project Management, 8, 119–132. https://doi.org/10.5267/j.jpm.2022.11.002

AlMeraj, Z., Alenezi, A. K., & Manuel, P. D. (2023). An empirical investigation into organisation cyber security readiness from the IT employee and manager perspectives. Electronic Government, 19(5), 539–559. https://doi.org/10.1504/EG.2023.133092

Alqahtani, M. S., & Erfani, E. (2021). Exploring the relationship between technology adoption and cyber security compliance: A quantitative study of UTAUT2 model. International Journal of Electronic Government Research, 17(4), 40-62. https://doi.org/10.4018/IJEGR.2021100103

Alraja, M. N., Hammami, S., Chikhi, B., & Fekir, S. (2016). The influence of effort and performance expectancy on employees to adopt e-government: Evidence from Oman. International Review of Management and Marketing, 6(4), 930-934.

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, 10(5), 4937-4955. http://doi.org/10.11591/ijece.v10i5.pp4937-4955

Arundel, A. (2023). *How to design, implement, and analyse a survey.* Edward Elgar Publishing.

Ashari, N. M., & Farouk, A. F. (2023). Exploring barriers and pathways towards Sarawak 2030 skills condition: A causal layered analysis. Futures, 145, 103079. https://doi.org/10.1016/j.futures.2022.103079

Avina, G. E., Gordon, S., Kittinger, R., Lakkaraju, K., & McCann, I. (2017). *Tailoring of cyber security technology adoption practices for operational adoption in complex organizations.* Albuquerque, New Mexico: Sandia Report

Ayaz, A., & Yanartas, M. (2020). An analysis on the Unified Theory of Acceptance and Use of Technology Theory (UTAUT): Acceptance of electronic document management system (EDMS). Computers in Human Behavior Reports, 2, 100032. https://doi.org/10.1016/j.chbr.2020.100032

Aytekin, A., Ozkose, H., & Ayaz, A. (2022). Unified Theory of Acceptance and Use of Technology (UTAUT) in mobile learning adoption: Systematic literature review and bibliometric analysis. Collnet Journal of Scientometrics and Information Management, 16(1), 75-116. https://doi.org/10.1080/09737766.2021.2007037

Belsley, D. A. (1991). *Conditioning diagnostics: Collinearity and weak data in regression.* John Wiley & Sons.

Benjamin, L. B., Adegbola, A. E., Amajuoyi, P., Adegbola, M. D., & Adegbola, K. B. (2024). Digital transformation in SMEs: Identifying cybersecurity risks and developing effective mitigation strategies. Global Journal of Engineering and Technology Advances, 19(2), 134-153. https://doi.org/10.30574/gjeta.2024.19.2.0084

Berlilana, Noparumpa, T., Ruangkanjanases, A., Hariguna, T., & Sarmini. (2021). Organization benefit as an outcome of organizational security adoption: The role of cyber security readiness and technology readiness. Sustainability, 132, 13761. https://doi.org/10.3390/su132413761

Bharathi, S. V. (2019). Forewarned is forearmed: Assessment of IoT information security risks using analytic hierarchy process. Benchmarking: An International Journal, 26(8), 2443– 2467. https://doi.org/10.1108/BIJ-08-2018-0264

Bland, E., Changchit, C., Changchit, C., Cutshall, R., & Pham, L. (2024). Investigating the components of perceived risk factors affecting mobile payment adoption. Journal of Risk and Financial Management, 17(6), 216. https://doi.org/10.3390/jrfm17060216

Boomer, W. H., Rana, S., & Milevoj, E. (2022). A meta-analysis of ewallet adoption using the UTAUT model. International Journal of Bank Marketing, 40(4), 791-819. https://doi.org/10.1108/IJBM-06-2021-0258

Budhathoki, T., Zirar, A., Njoya, E. T., & Timsina, A. (2024). ChatGPT adoption and anxiety: A cross-country analysis utilising the Unified Theory of Acceptance and Use of Technology (UTAUT). Studies in Higher Education, 49(5), 831–846. https://doi.org/10.1080/03075079.2024.2333937

Buraimoh, O. F., Boor, C. H. M., & Aladesusi, G. A. (2023). Examining facilitating condition and social influence as determinants of secondary school teachers' behavioural intention to use mobile technologies for instruction. Indonesian Journal of Educational Research and Technology, 3(1), 25-34. https://doi.org/10.17509/ijert.v3i1.44720

Camilleri, M. A. (2024). Factors affecting performance expectancy and intentions to use ChatGPT: Using SmartPLS to advance an information technology acceptance framework. Technological Forecasting and Social Change, 201, 123247. https://doi.org/10.1016/j.techfore.2024.123247

Catherine, N., Geofrey, K. M., Moya, M. B., & Aballo, G. (2017). Effort expectancy, performance expectancy, social influence and facilitating conditions as predictors of behavioural intentions to use ATMs with fingerprint authentication in Ugandan Banks. Global Journal of Computer Science and Technology: E Network, Web and Security, 17(5), 5-22.

Chai, L. G. (2022). The next frontier towards digital Sarawak: Advancing into the future. In M. N. Almunawar, M. Z. Islam & P. O. de Pablos (Eds.), *Digital transformation management challenges and futures in the Asian digital economy* (pp.247-265). Routledge.

Chapman, T. A., & Reithel, B. J. (2021). Perceptions of cybersecurity readiness among workgroup IT managers. Journal of Computer Information Systems, 61(5), 438–449. https://doi.org/10.1080/08874417.2019.1703224

Chin, W. W. (2010). How to write up and report PLS analyses. In: Esposito Vinzi, V., Chin, W., Henseler, J. & Wang, H. (eds.), *Handbook of Partial Least Squares. Springer handbooks of computational statistics* (pp. 655-690). Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-32827-8_29

Choi, M., Lee, J., & Hwang, K. (2018). Information systems security (ISS) of e-government for sustainability: A dual path model of ISS influenced by institutional isomorphism. Sustainability, 10(5), 1555. https://doi.org/10.3390/su10051555

Creazza, A., Colicchia, C., Spiezia, S., & Dallari, F. (2022). Who cares? Supply chain managers' perceptions regarding cyber supply chain risk management in the digital transformation era. Supply Chain Management: An International Journal, 27(1), 30–53. https://doi.org/10.1108/SCM-02-2020-0073

CyberSarawak (2024). About Cyber Sarawak. https://www.cybersarawak.gov.my/web/about_us/overview/

Dalati, S., & Gomez, J. M. (2018). Surveys and questionnaires. In J. M. Gomez & S. Mouselli (Eds.), *Modernizing the academic teaching and research environment* (pp. 175-186). Springer Nature Link.

Dash, G. & Paul, J. (2021). CB-SEM vs PLS-SEM methods for research in social sciences and technology forecasting. Technological Forecasting and Social Change, 173, 121092. https://doi.org/10.1016/j.techfore.2021.121092

Ebenezer, A. E., & Piate, R. S. (2023). Assessment of different methods of sampling techniques: The strengths and weakness. Shared Seasoned International Journal of Topical Issues, 9(1), 64-83.

Engotoit, B., Kituyi, G. M., & Moya, M. B. (2016). Influence of performance expectancy on commercial farmers' intention to use mobile-based communication technologies for agricultural market information dissemination in Uganda. Journal of Systems and Information Technology, 18(4), 346–363. https://doi.org/10.1108/JSIT-06-2016-0037

Etim, E., & Daramola, O. (2023). Investigating the e-readiness of informal sector operators to utilize web technology portal. Sustainability, 15, 3449. https://doi.org/10.3390/su15043449

Falk, R. F., & Miller, N. B. (1992). *A primer for soft modeling.* University of Akron Press.

Falowo, I., Opoola, S., Riep, J., Adewopo, V. A., & Koch, J. (2022). Threat actors' tenacity to disrupt: Examination of major cybersecurity incidents. IEEE Access, 10, 134038–134051. https://doi.org/10.1109/ACCESS.2022.3231847

Friday, N., & Leah, N. (2024). Types of purposive sampling techniques with their examples and application in qualitative research studies. British Journal of Multidisciplinary and Advanced Studies, 5(1), 90-99. https://doi.org/10.37745/bjmas.2022.0419

Garba, A. A., & Bade, A. M. (2021). The current state of cybersecurity readiness in Nigeria organizations. International Journal of Multidisciplinary and Current Educational Research, 3(1), 154-162.

Ghanad, A. (2023). An overview of quantitative research methods. International Journal of Multidisciplinary Research and Analysis, 6(8), 3794-3803. https://doi.org/10.47191/ijmra/v6-i8-52

Goretzko, D., Siemund, K., & Sterner, P. (2024). Evaluating model fit of measurement models in confirmatory factor analysis. Educational and Psychological Measurement, 84(1), 123-144. https://doi.org/10.1177/00131644231163813

Hair, J. F., Sarstedt, M., Hopkins, L., & Kuppelwieser, V. G. (2014). Partial least squares structural equation modeling (PLS-SEM): An emerging tool in business research. European Business Review, 26(2), 106–121. https://doi.org/10.1108/EBR-10-2013-0128

Hair, J. F., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2017), *A primer on Partial Least Squares Structural Equation Modeling (PLS-SEM), 2nd ed.,* Sage, Thousand Oaks, CA.

Hair, J. F., Hult, G. T. M., Ringle, C. M., Sarstedt, M., Danks, N. P., & Ray, S. (2021). Evaluation of reflective measurement models. In: *Partial Least Squares Structural Equation Modeling (PLS-SEM) using r. Classroom companion: Business* (pp. 75-90). Springer, Cham. https://doi.org/10.1007/978-3-030-80519-7_4

Hakiem, N., Afrizal, S., Shofi, I. M., Wardhani, L. K., Anggraini, N., Zulhuda, S., & Setiadi, Y. (2023). Assessing cybersecurity readiness among higher education institutions in Indonesia using management perspectives. ICIC Express Letters, 17(10), 1151-1158. https://doi.org/10.24507/icicel.17.10.1151

Hamarah, C. M., & Mohamad, F. S. (2020). Mathematical cognition and big data analytics: Are Sarawak teachers ready? Journal of Cognitive Sciences and Human Development, 6(1), 12-19. https://doi.org/10.33736/jcshd.1591.2020

Hanif, Y., & Lallie, H. S. (2021). Security factors on the intention to use mobile banking applications in the UK older generation (55+). A mixed-method study using modified UTAUT and MTAM - with perceived cyber security, risk, and trust. Technology in Society, 67, 101693. https://doi.org/10.1016/j.techsoc.2021.101693

Hasan, S., Ali, M., Kurnia, S., & Ramayah, T. (2021). Evaluating the cyber security readiness of organizations and its influence on performance. Journal of Information Security and Applications, 58(4), 102726. https://doi.org/10.1016/j.jisa.2020.102726

Hasani, T., Rezania, D., Levallet, N., O'Reilly, N., & Mohammadi, M. (2023). Privacy enhancing technology adoption and its impact on SMEs' performance. International Journal of Engineering Business Management, 15. https://doi.org/10.1177/18479790231172874

Hasbie, S. N. R., Assim, M. I., Taasim, S. I., & Mahdi, A. K. (2023). Information and communication technology and behavioral intention: A review paper. International Journal of Academic Research in Business and Social Sciences, 13(9), 1112-1120. https://doi.org/10.6007/IJARBSS/v13-i9/17996

Henseler, J., Hubona, G., & Ray, P. A. (2015). Using PLS path modeling in new technology research: Updated guidelines. Industrial Management and Data Systems, 116(1), 2-20. https://doi.org/10.1108/IMDS-09-2015-0382

Hilowle, M., Yeoh, W., Gorbler, M., Pye, G., & Jiang, F. (2022). National digital identity systems: Human-centric cybersecurity review. Journal of Computer Information Systems, 63(5), 1264–1279. https://doi.org/10.1080/08874417.2022.2140089

Hu, L.T., & Bentler, P. M. (1999). Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. Structural Equation Modeling, 6(1), 1-55. https://doi.org/10.1080/10705519909540118

Jamil, H., Zia, T., Nayeem, T., Whitty, M. T., & D'Alessandro, S. (2024). Human-centric cyber security: Applying protection motivation theory to analyse micro business owners' security behaviours. Information and Computer Security, ahead-of-print. https://doi.org/10.1108/ICS-10-2023-0176

Jugah, I., Chai, S. Y., Yusaf, N. A., Alfred, O., & Sawai, A. (2022). Public readiness and acceptance towards implementation of Sarawak digital economy: A case study in Kuching, Sarawak. Journal of Administrative Science, 19(2), 109-118.

Kalakuntla, R., Vanamala, A. B., & Kolipyaka, R. R. (2019). Cyber security. HOLISTICA – Journal of Business and Public Administration, 10(2), 115-128. https://doi.org/10.2478/hjbpa-2019-0020

Kazemi, A., Golkar, M. K., & Lajmiri, S. (2023). Origins of cyber security: Short report. International Journal of Reliability, Risk and Safety: Theory and Application, 6(2), 77-83. https://doi.org/10.22034/IJRRS.2023.6.2.9

Khan, S., Khan, N., Rahman, H. M., & Tan, S. L. (2024). Malaysia's commitment to establishing a digital transformation-friendly ecosystem shows its determination to become a regional digital leader. Peace and Conflict, 30(2), 40-56.

Kock, F., Berbekova, A., & Assaf, G. A. (2021). Understanding and managing the threat of common method bias: Detection, prevention and control. Tourism Management, 86, 104330. https://doi.org/10.1016/j.tourman.2021.104330

Kock, N. (2015). Common method bias in PLS-SEM: A full collinearity assessment approach. International Journal of e-Collaboration, 11(4), 1-10. https://doi.org/10.4018/ijec.2015100101

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

Kumar, S., Verma, A. K., & Mirza, A. (2024). Digitalisation, artificial intelligence, IOT, and industry 4.0 and digital society. In: *Digital transformation, artificial intelligence and society. Frontiers of artificial intelligence, ethics and multidisciplinary applications.* Springer, Singapore. https://doi.org/10.1007/978-981-97-5656-8_3

Lahcen, R. A. M., Caulkins, B., Mohapatra, R., & Kumar, M. (2020). Review and insight on the behavioral aspects of cybersecurity. Cybersecurity, 3(10). https://doi.org/10.1186/s42400-020-00050-w

Li, W. (2021). The role of trust and risk in citizens' e-government services adoption: A perspective of the extended UTAUT Model. Sustainability, 13(14), 7671. https://doi.org/10.3390/su13147671

Lim, W. M. (2022). Toward a Theory of Social Influence in the new normal. Activities, Adaptation & Aging, 46(1), 1-8. https://doi.org/10.1080/01924788.2022.2031165

Listiyani, S. R., & Princes, E. (2024). The Unified Theory of Acceptance and use of Technology (UTAUT) Model on the quality of employee information service sites and learning centers at Xyz Company. Journal of System and Management Sciences, 14(10), 333-349. https://doi.org/10.33168/JSMS.2024.10xx

Liu, N., Nikitas, A., & Parkinson, S. (2020). Exploring expert perceptions about the cyber security and privacy of connected and autonomous vehicles: A thematic analysis approach. Transportation Research Part F: Traffic Psychology and Behaviour, 75, 66-86. https://doi.org/10.1016/j.trf.2020.09.019

Mahdi, A. F., Lajim, S. F., Ibrahim, A. F., & Zin, M. Z. (2019). E-readiness indicators among individual on Sarawak digital economy. Borneo International Journal, 2(1), 1-4.

Mansour, A. T., Ibrahim, H., & Hassan, S. (2021). The behavioral intention's role: Facilitating condition and use of e-government services among SMEs in Saudi Arabia. Turkish Journal of Computer and Mathematics Education, 12(1), 1520-1528.

Marsintauli, F., Diennia, R. N., & Sujarminto, A. (2023). Applying the UTAUT to understand factors affecting the use of Indonesia public administration. E3S Web of Conferences, 388, 04049. https://doi.org/10.1051/e3sconf/202338804049

Memon, M. A., Ramayah, T., Cheah, J. H., Ting, H., Chuah, F., & Cham, T. H. (2021). PLS-SEM statistical programs: A review. Journal of Applied Structural Equation Modeling, 5(1), i-xiv. https://doi.org/10.47263/JASEM.5(1)06

Mensah, I. K., & Khan, M. K. (2024). Unified Theory of Acceptance and Use of Technology (UTAUT) model: Factors influencing mobile banking services' adoption in China. SAGE Open, 14(1). https://doi.org/10.1177/21582440241234

Muller, S. R., & Lind, M. L. (2020). Factors in information assurance professionals' intentions to adhere to information security policies. International Journal of Systems and Software Security and Protection, 11(1), 17-32. https://doi.org/10.4018/IJSSSP.2020010102

Neri, M., Niccolini, F., & Martino, L. (2023). Organizational cybersecurity readiness in the ICT sector: A quanti-qualitative assessment. Information & Computer Security, 32(1), 38-52. https://doi.org/10.1108/ICS-05-2023-0084

Putra, A. R., Musnadi, S., & Chan, S. (2019). Analysis of behavioral intention to use a community-based information system in the city of Banda Aceh, Indonesia. Expert Journal of Marketing, 7(2), 93-99.

Rajendran, K., & Jayakrishnan, J. (2018). Consumer perceived risk in car purchase. ICTACT Journal on Management Studies, 4(2), 736-741. https://doi.org/10.21917/ijms.2018.0100

Rattanapong, P., & Ayuthaya, S. D. (2025). Influential factors of cybersecurity investment: A quantitative SEM analysis. Management Science Letters, 15, 31–44. https://doi.org/10.5267/j.msl.2024.3.005

Rehman, M., Esichaikul, V., & Kamal, M. (2012). Factors influencing e-government adoption in Pakistan. Transforming Government: People, Process and Policy, 6(3), 258–282. https://doi.org/10.1108/17506161211251263

Rizakalla, N., Tannady, H., & Bernando, R. (2024). Analysis of the influence of performance expectancy, effort expectancy, social influence, and attitude toward behavior on intention to adopt live.on. Multidisciplinary Reviews, 6, 2023spe017. https://doi.org/10.31893/multirev.2023spe017

Safa, N. S., Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. Computers and Security, 56, 70-82. https://doi.org/10.1016/j.cose.2015.10.006

Sageng, C. W., Kasa, M., Pudun, J. M., & Ramli, N. (2020). Sarawak cuisine: An overview and its identity. Journal of Tourism, Hospitality & Culinary Arts, 12(3), 15-30.

Salimon, M. G., Mokhtar, S. S. M., Yusoff, R. Z., Adeleke, A. Q., Morakinyo, S., & Mushi, H. M. (2017). Facilitating conditions and perceived security as antecedents of trust among e-banking customers in Nigeria. International Journal of Economic Research, 14(19), 265-276.

Sarawak Multimedia Authority (2023). Sarawak Digital Economy Blueprint 2030. https://www.sma.gov.my/web/attachment/show/?docid=amI0Y1FsaWo5MFp6ZWdwMG5rL242UT09OjrW9vijjeXQPzhr0B0hGIo7.

Seemma, P. S., Nandhini, S., & Sowmiya, M. (2018). Overview of cyber security. International Journal of Advanced Research in Computer and Communication Engineering, 7(11), 125-128. https://doi.org/10.17148/IJARCCE.2018.71127

Sekak, S. N., Sazali, S. M., Akbar, A. R., & Junus, Y. (2022). Challenges and opportunities towards industrial Revolution 4.0 (IR 4.0) among contractors in Malaysia construction industry. Jurnal Penyelidikan Sains Sosial, 5(17), 42-49. https://doi.org/10.55573/JOSSR.051704

Serojai, A. T. B., Ujir, H. B., & Hipiny, I. H. B. M. (2021). E-commerce readiness assessment in Sarawak. Acta Informatica Pragensia, 10(2), 192-206. https://doi.org/10.18267/j.aip.153

Sivarethinamohan, R., & Sujatha, S. (2021). Behavioral intentions towards adoption of information protection and cyber security (email security and online privacy): SEM model. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 12(6), 56-68. https://doi.org/10.17762/turcomat.v12i6.1267

Sulaiman, S., & Halamy, S. (2021). ICT education as a catalyst to bridge digital divide: The roles of UiTM Sarawak in rural areas. International Journal of Advanced Research in Education and Society, 3(2), 174-181.

Supayah, G., & Ibrahim, J. (2016). An overview of cyber security in Malaysia. Kuwait Chapter of Arabian Journal of Business and Management Review, 6(4), 12-20. https://doi.org/10.12816/0036698

Szwajca, D. (2019). Digital customer as a creator of the reputation of modern companies. Foundations of Management, 11(1), 255-266. https://doi.org/10.2478/fman-2019-0021

Taherdoost, H. (2022). Cybersecurity vs. information security. Procedia Computer Science, 215, 483–487. https://doi.org/10.1016/j.procs.2022.12.050

Tang, M. B., Dieo, B., Suhaimi, K., & Andam, J. (2022). The emergence of e-wallet in Sarawak: Factors influencing the adoption of Sarawak Pay. International Journal of Business and Society, 23(3), 1423-1442. https://doi.org/10.33736/ijbs.5172.2022

The official portal of Sarawak Government (2024). Sarawak population. https://sarawak.gov.my/web/home/article_view/240/175/.

Uher, V., Drazdilova, P., Platos, J., & Badura, P. (2022). Automation of cleaning and ensembles for outliers detection in questionnaire data. Expert Systems with Applications, 206, 117809. https://doi.org/10.1016/j.eswa.2022.117809

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. MIS Quarterly, 27(3), 425-478. https://doi.org/10.2307/30036540

Wang, X., & Cheng, Z. (2020). Cross-sectional studies: Strengths, weaknesses, and recommendations. CHEST, 158(1), S65-S71. https://doi.org/10.1016/j.chest.2020.03.012

Whittaker, T. A., & Noteboom, C. (2019). Factors influencing curriculum adoption in undergraduate cybersecurity programs. Issues in Information Systems, 20(3), 64-73. https://doi.org/10.48009/3_iis_2019_64-73

Xue, L., Rashid, A. M., & Ouyang, S. (2024). The Unified Theory of Acceptance and Use of Technology (UTAUT) in higher education: A systematic review. Sage Open, 14(1). https://doi.org/10.1177/21582440241229570

Yong, M. L., Hamid, N. A., & Lee, T. C. (2020). Is Malaysia ready for Industry 4.0? Issues and challenges in manufacturing industry. International Journal of Integrated Engineering, 12(7), 134-150. https://doi.org/10.30880/ijie.2020.12.07.016

Zadha, H. A., & Suparna, G. (2023). The role of brand trust mediates the effect of perceived risk and brand image on intention to use digital banking service. American Journal of Humanities and Social Sciences Research, 7(1), 161-175

Zahiroh, M. Y. (2020). Cybersecurity awareness and digital skills on readiness for change in digital banking. Li Falah Jurnal Studi Ekonomi dan Bisnis Islam, 5(2), 53-73. https://doi.org/10.31332/lifalah.v5i2.2271

Zeng, N., Liu, Y., Gong, P., Hertogh, M., & Konig, M. (2021). Do right PLS and do PLS right: A critical review of the application of PLS-SEM in construction management research. Frontiers of Engineering Management, 8(3), 356–369. https://doi.org/10.1007/s42524-021-0153-5