

Developing a Cyber Trust Model for Strengthening Cybersecurity in Malaysia's Digital Economy: A Qualitative Theory-Building Study

Aumuhaimi binti Md Yusof^{*1}, Muhamad Khairulnizam bin Zaini, Irni Eliana binti Khairuddin

¹*Faculty of Information Science, Univeriti Teknologi MARA, UiTM Selangor, 40150 Shah Alam, Malaysia*

ARTICLE INFO

Article history:

Received 1 Jun 2026

Revised 25 August 2026

Accepted 5 September 2026

Published 0 October 2026

Keywords:

Digital trust

Cybersecurity

Digital economy

Qualitative research

Thematic analysis;

Cyber Trust Model

ABSTRACT

As Malaysia's digital economy continues to rapidly develop, companies are now more vulnerable to cyber threats. Previous research has primarily been centred on technical control and risk management and has not been as much on trust as a basis of secure digital business environments. This study aims to bridge this void by creating a Cyber Trust Model which defines the critical factors that influence cybersecurity resilience and digital trust in the digital economy in Malaysia through a series of interviews with ten government, critical and private sector cybersecurity practitioners. This analysis revealed four dimensions that are interrelated: Cybersecurity Challenges, Governance and Organizational Competence, Technology Security Measures, and Digital Trust Antecedents. The study demonstrates that, besides security measures, the factors for digital trust include leadership commitment, regulatory adherence, continuous risk management processes, employee awareness, transparency, privacy protection and stakeholder confidence. The model combines technical, organizational, governance and human components to go beyond the traditional and technology-focused cybersecurity approach and is based on the institutional environment in Malaysia. Cyber Trust Model gives policymakers, cybersecurity practitioners and digital business leaders a practical approach to the development of digital trust and the creation of a more secure digital transformation and organizations that are more resilient. It provides an empirical foundation for further research into cyber trust and cybersecurity governance, and provides a measure that an organization can apply to its own to diagnose and improve its resilience. With the rapid development of Malaysia's digital economy, it is vital to ensure that trust-based, comprehensive cybersecurity practice is firmly rooted, so as to maintain the security and resilience of the digital economy.

<https://doi.org/10.24191/140tsf68>

INTRODUCTION

Digital technology has had an unprecedented transformation of the global economy impacting on the way governments, organisations and people communicate, interact and create value. The acceleration of digital transformation is tied to a group of enabling technologies, like cloud computing, artificial intelligence (AI), big data analytics, blockchain, the Internet of Things (IoT) and mobile applications that

¹ * Corresponding author. *E-mail address:* 2022883136@student.uitm.edu.my
<https://doi.org/10.24191/140tsf68>

have helped companies become more efficient, better customer service, and offering new digital services (Vial, 2019; Verhoef et al., 2021). The digital economy is one of the key drivers of growth, competitiveness and innovation in the path of sustainable digital transformation (OECD, 2024; World Bank, 2021) for emerging economies.

The Malaysia Digital Economy Blueprint (MyDIGITAL), the Twelfth Malaysia Plan (12MP) and the Malaysia Cyber Security Strategy 2020-2024 are some of the strategic initiatives that reflect the government's commitment to this path in Malaysia. In concert, all these efforts are anticipated to contribute to the improvement of the digital infrastructure, increase technology innovation and continue to strengthen the contribution of the digital economy to national development (Malaysia Digital Economy Corporation [MDEC], 2021; Economic Planning Unit, 2021).

Digital technology has revolutionized the lives and working practices of societies, and connected governments, financial service providers, health services, education and business in a more interconnected online world. This connectivity has facilitated the access to essential services such as online banking, e-commerce, electronic payments for bills and has enabled the provision of e-government services and smart manufacturing. (United Nations, 2024; OECD, 2024). But, this symbiotic relationship has made organizations more susceptible to greater and more formidable cyber attacks. Their impact is now reaching far beyond degraded systems to impact on the continuity of businesses, economic stability, organizational reputations, and national security, in some instances (World Economic Forum [WEF], 2024; National Institute of Standards and Technology [NIST], 2024).

Worldwide, there are more and more complex cyberattacks. The events have demonstrated that cyber security is not an IT problem anymore, it is a strategic problem of the organization that needs to foster good governance, leadership and enterprise-wide risk management (NIST, 2024; WEF, 2024). The digital transformation is happening in all industries, in both public or private sectors and Malaysia is no exception. Digital assets are universally at risk of cyber-attack, with critical national infrastructure and financial institutions, healthcare providers, educational organisations and digital companies being the primary targets to compromise the confidentiality, integrity and availability of digital assets (CyberSecurity Malaysia, 2024; NIST, 2024).

A security breach's impact is far more than just monetary. Disruption, intellectual property theft, regulatory fines and penalties, legal liability and lasting reputation damage are among the challenges faced by organisations (IBM Security, 2024; Ponemon Institute, 2024). Perhaps most notably, these failures can affect the trust of users in digital services, and prompt them to be more skeptical about sharing sensitive information, making online transactions, and using digital services more generally. Trust has thus emerged as a critical precondition for the effective integration of digital transformation: Users are increasingly looking to the digital world for organizations that act securely, with good faith and transparency before agreeing to interact with them (Confente et al., 2023; OECD, 2024). Cybersecurity and digital trust have thus been intertwined concepts that impact the sustainability of digital business ecosystems in the long-term (OECD, 2024; Confente et al., 2023).

Digital trust is trust in digital technology and online services that they operate reliably, honestly and transparently (OECD, 2024; Deloitte, 2023). Creating this trust depends on the organizations' ability to put in place effective procedures for safeguarding personal information and data (ISO/IEC, 2022; NIST, 2024), as well as accountability and regulatory compliance (OECD, 2024). The more aligned the expectations of the organisations and the users are, the higher the likelihood of the use of digital services, such as online

banking and shopping, as reported by Confente et al. (2023) and Gefen et al. (2003). Conversely, if the organisation suffers a series of cyber incidents, then that trust is lost and the organisation may no longer avail the services affecting its competitiveness. It is therefore imperative to embed trust building in cybersecurity strategies and digital growth programs to help build and sustain trust among users and the ongoing digital transformation (OECD, 2024).

Importantly, digital trust is not just about technical measures – it is about how organisations behave, namely, how they are transparent, ethical and take responsibility in their management and protection of user information (Mayer et al., 1995). Organisations which adopt these principles make digital services safe for users to engage with and are beneficial to the users and providers. Digital technologies are evolving and the ability to create and maintain digital trust will likely be a key determinant of organisational competitiveness and success in the digital economy, whether they are on the winning side or losing side of the race (Deloitte, 2023; OECD, 2024).

While there has been a significant amount of research in the cybersecurity field, most of the research has been directed toward the technological aspect of security controls, cybersecurity frameworks, risk assessment methods, incident response processes and information security standards (Taherdoost, 2022; von Solms & van Niekerk, 2013). There are established frameworks to assist in the conversation of cybersecurity risk management and securing an organization, including the NIST Cybersecurity Framework (CSF 2.0), ISO/IEC 27001, and Zero Trust Architecture that provide a common language (NIST, 2024; ISO/IEC, 2022). However, these methods are more likely to be technical, governance, and regulatory oriented, with minimal attention paid to the factors of trust that impact the role of cybersecurity in digital business environments (Dhillon et al., 2021; NIST, 2024).

There is a parallel line of research that has investigated the factors that lead users to trust websites and online businesses in other contexts, such as online shopping and disclosing personal information (Gefen et al., 2003; McKnight et al., 2011). But, little work has been conducted on the link between trust and cyber security practice and how it affects cyber security related organizational resilience, especially in the case of the digital economy in Malaysia as it is still in infancy (Dhillon et al., 2021; Alshaikh et al., 2022). There are not many studies that focus on the trust building activities of cybersecurity practitioners, on the factors that underpin trust, or on how these factors could be turned into a structure to enhance the cyber security resilience of an organization (Siponen & Vance, 2020; Alshaikh et al., 2022). However, models developed to explain an individual consumer's decision to make a one-off purchase from a website focus on perceived benevolence, ability and integrity of the vendor, as the antecedents of the adoption of a single website purchase (McKnight et al., 2002; Gefen et al., 2003). They are not intended to represent the overall ability of an organization to be cyber secure over time, across multiple stakeholders, through governance, employee behavior, and technology, but rather the lack of a “single user trust judgement” in any individual user that this study seeks to bridge.

Therefore, the issue of digital trust needs to be understood within the context of cybersecurity and the underlying factors of trust and how they can be used to create a coherent theoretical construct (OECD, 2024; Dhillon et al. 2021). This would further add to the knowledge of digital trust and provide practical value to augment cybersecurity governance and organizational resilience (Alshaikh et al., 2022; Dhillon et al., 2021).

This study thus takes a qualitative approach to create a Cyber Trust Model based on the experiences and professional insights of cybersecurity practitioners in Malaysia, addressing these shortcomings. Instead

of testing the existing theories based on quantitative measures, as many studies have been, this is a qualitative approach with in-depth thematic analysis. The ten (10) cybersecurity professionals were interviewed in government agencies, critical infrastructure, and private organizations, and the data analysed thematically with a six-phase approach to identify the patterns, categories and themes emerging from the data (Braun & Clarke, 2022).

The results suggest that cybersecurity is becoming a more than just technical service, but a part of organizational competency, that involves organizational governance, leadership, technological capability, employee awareness, regulatory compliance, organizational culture, and stakeholder engagement. In this context, cyber security plays a vital role in the digital trust, resilience of organisations and sustainable digital transformation of Malaysia's digital economy (Dhillon et al., 2021; Alshaikh et al., 2022). This broader view will likely give a firmer basis for continuing the digital development of the nation.

Based on these empirical results, an interrelated Cyber Trust Model is proposed consisting of the four dimensions of Cyber Trust (Technological, Organizational, Governance, and Human aspects). The model has been constructed to attempt to answer the following questions:

- (i) RQ1: What are the cybersecurity problems of the trust-specific problems in the digital economy ecosystem?
- (ii) RQ2: What digital trust factors could be antecedents to tackle cybersecurity issues in the digital ecosystem?
- (iii) RQ3: What technological components are required to integrate into a digital trust framework that is based on cybersecurity?
- (iv) RQ4: What are the possible impacts of a cybersecurity-driven digital trust framework in addressing security issues in Malaysia's digital businesses?

This study is related to the theory and practice in a number of ways. In theory, it adds to the current knowledge base on cybersecurity and digital trust as a whole by bringing together cybersecurity governance, cybersecurity technology protections, organizational capabilities, and cyber trust-building mechanisms under an integrated conceptual framework (Dhillon et al., 2021; Alshaikh et al., 2022). The methodology of the paper highlights the use of qualitative theory development using expert interviews and thematic analysis via ATLAS.ti software (Braun & Clarke, 2022; Myers, 2020). The proposed Cyber Trust Model is one that could be implemented by policymakers, government agencies, cybersecurity practitioners and cybersecurity organizational leaders in practice in Malaysia to improve the governance of cybersecurity, enhance confidence of stakeholders, create organizational resilience and enable sustainable digital transformation within the ever-changing digital economy of Malaysia (NIST, 2024; OECD, 2024; MDEC, 2021).

STATEMENT OF THE PROBLEMS AND RATIONALE FOR THE STUDY

The digital economy has emerged as a key driver of economic growth, innovation, and national competitiveness worldwide (Organisation for Economic Co-operation and Development [OECD], 2024; World Bank, 2021). The adoption of digital technologies has been gaining momentum across the public and private sectors in Malaysia, including cloud computing, artificial intelligence (AI), the Internet of Things (IoT), blockchain, digital financial services and even e-commerce, through various government initiatives (Malaysia Digital Economy Blueprint [MyDIGITAL]; Economic Planning Unit, 2021). These technological advances have helped increase organizational productivity and enabled effective support for

the provisioning of digital services (Vial, 2019; Verhoef et al., 2021), but have also contributed to the overall cyber threat landscape and started to pose risks to firms because of their increasing sophistication (World Economic Forum [WEF], 2024; National Institute of Standards and Technology [NIST], 2024).

Regardless of whether it's the government, a financial institution, a healthcare organization, an educational institution or a digital company, cyber incidents are becoming more common and complex. Today, threats like ransomware, phishing, malware, distributed denial-of-service (DDoS) attacks, insider threats and data breaches regularly impact businesses, causing financial damage, reputational damage, regulatory consequences, and eroding trust in the public (Bada et al., 2019; WEF, 2024; IBM Security, 2024). With increasing reliance on digital infrastructure, cybersecurity has evolved from a purely technical issue to a strategic organizational ability that can impact business continuity, resilience and future competitiveness (NIST, 2024; Dhillon et al., 2021).

Among the things that can strike fear into heart of those thinking about a cyber breach is the loss of trust on any digital system. This is because digital trust is the ability of organisations to operate technology, data and online interactions securely, reliably, ethically and transparently (Organization for Economic Co-operation and Development [OECD] 2024; Mayer et al. 1995). According to the OECD in 2024, one of the major pillars of the digital transformation is trust. The sense of confidence and trustfulness in the digital environment strengthens digital engagement, sharing of personal information and digital transactions (OECD, 2024). However, with a cyber security incident, it can have significant implications for the loss of trust in the system and diminish engagement in digital activities. This can also affect an organization's reputation (Confente et al., 2023; WEF, 2024). This is a major concern that consumers have now. Hence, it is crucial for organisations to focus on digital trust and ensure they do not fall victim to cyber security breaches to keep their stakeholders trust and confident. This will help establish a trustworthy and safe digital environment, essential for digital transformation and online interactions.

With more and more dependence on technology, maintaining security of information is increasingly vital. The majority of research has focused on employing technology for regulating and administering cybersecurity such as adhering to standards and rules (Taherdoost, 2022; von Solms & van Niekerk, 2013). A guide to combat cyber threats such as ISO/IEC 27001 and the NIST Cybersecurity Framework. They are used to identify, prevent and solve issues and to restore to normalcy after a cyber incident (International Organization for Standardization [ISO], 2022; NIST, 2024). These standards tend to be more technical in nature and the ways to control them. The important thing that is missing is the rationale behind the importance of good leadership, understanding what employees are doing, being transparent, protecting employee privacy and gaining stakeholder trust. Combined, all this contributes to trust in digital spaces, a key component to safeguarding our information.

Many initial studies of digital trust have examined consumer trust in the context of ecommerce - the consumer's evaluation of the trustworthiness of a website, their actions in the Internet and their interpretation of their personal data security (Gefen et al., 2003; McKnight et al., 2011) and on technology acceptance (Venkatesh et al., 2003). However, less has been focused on the role of digital trust within organizations, specifically in terms of information security practices and cyber threat preparedness (CyTP) (Dhillon et al., 2021; Siponen & Vance, 2020), or the factors that enable the creation of such trust (Siponen, 2021). Further research is needed to better understand the methods by which organisations can gain the trust of their customers and partners, via cybersecurity capabilities and cybersecurity resilience, for instance (Alshaikh et al., 2022; Dhillon et al., 2021). This gap is significant in terms of the trust in the digital economy and its implications in general.

However, the study on cyber security is still limited and minimal particularly on the practitioners' experiences in Malaysia. While the nation has been pursuing efforts to enhance cybersecurity capacity via

policy initiatives and legislation, few in-depth qualitative studies have taken an in-depth look at realities of cybersecurity from a point of view that is directly impacted by it (CyberSecurity Malaysia, 2024; Malaysia Digital Economy Corporation [MDEC], 2021). In Malaysia, most of the previous studies have thus far adopted qualitative methods to verify existing theories developed in the field and/or to measure the state of cybersecurity maturity of the country (Rahim et al., 2022; Alshaikh et al., 2022). These approaches offer good broad-level understanding, but not as well suited to generating new understanding, or the realities of doing cybersecurity work on the ground (Myers, 2020; Creswell & Poth, 2018). However, the lack of understanding of the nature of trust in the Malaysian digital economy has limited the ability to develop an empirical-based approach to building an account of cyber trust and its implications for a secure digital economy (Dhillon et al., 2021; Alshaikh et al., 2022).

To appreciate the impact of cybersecurity practices on digital trust, it is necessary to have a way to capture the overall picture, namely a method that would allow to build theory from empirical observation rather than to test theory before it is developed (Myers, 2020; Eisenhart & Graebner, 2007). Working directly with practitioners and using their first-hand knowledge and experience to gain access to this understanding is particularly important (Braun & Clarke, 2022). This has steered the study towards understanding the fundamentals of digital trust, and the role of cybersecurity practices. As it aims to learn from cybersecurity experts from both industry and government, it eventually use these insights to build a comprehensive model of cyber trust to understand what can build trust in digital systems, and how digital systems can be made more secure and trustworthy (Braun & Clarke, 2022; Myers, 2020).

This study then designs a Cyber Trust Model that involves technical defenses, governance mechanisms and organizational capability and human factors to increase the cybersecurity resilience and digital trust in digital economy in Malaysia. Proposed model builds on previous literature in cyber security that has largely centered on the technological aspect of cyber security and viewed cyber trust as a multi-dimensional organizational capability. It also fits with the digital trust theory since it offers an empirically-derived model using the thematic analysis of practitioners' experience (Braun & Clarke, 2022; Myers, 2020). For example, the stakeholders who are involved in the policy, regulatory, cybersecurity and organizational leadership can use this model as a strategic reference to strengthen cybersecurity governance, build trust and confidence among the stakeholders, support sustainable digital transformation and enhance cyber resilience in an organisation against cyber threats. Thus, the model can be used as a practical tool for policy makers, regulators, cybersecurity professionals, and cyber-resilience leaders of organizations to strengthen cybersecurity governance, build stakeholder trust and confidence, support for sustainable digital transformation and enhance cyber-resilience of organizations against cyber threats (NIST, 2024; OECD, 2024; WEF, 2024).

OBJECTIVE

This paper is to create and validate a Cyber Trust Model based on the professional knowledge and experience of cybersecurity practitioners in Malaysia digital economy. Specifically, the study aims to: (i) define the cybersecurity issues most closely linked to digital trust problems; (ii) define the cybersecurity aspects that would alleviate such issues; (iii) outline the technology aspects that a Cybersecurity-based Digital Trust framework should include; and (iv) discuss the application of the Digital Trust framework to address the security issues faced by the Malaysian Digital businesses. The goals for these are addressed through qualitative thematic analysis of semi-structured interviews with cybersecurity practitioners and the resulting model is designed to be a practical diagnostic and planning tool for organisations, regulators and policy makers looking to improve digital trust while enhancing cybersecurity capability.

METHODOLOGY

In Malaysia, where cybersecurity risk is growing, there is a critical need to trust in the digital economy. To investigate the factors influencing cyber trust, this study followed a qualitative, theory building methodology (Myers, 2020; Eisenhardt & Graebner, 2007) and used purposive sampling to invite ten (10) cybersecurity professionals from government agencies and private companies who have significant expertise in cybersecurity and digital transformation (Patton, 2015; Saunders et al., 2018). The researcher applied a semi-structured interview method to tap participants' perspectives and experiences regarding cybersecurity issues, digital trust and practice in organization (Kallio et al., 2016; Myers, 2020). The ten informants were from three different sectors, with an average of three informants per sector, but the number of informants was not the only criterion used to assess the process of saturation; iterative, cross-sector constant comparison was used as an additional methodology to determine saturation, as later interviews (in the smallest sector represented) produced no qualitatively new codes, but instead reinforced or expanded categories already existing in the coding frame (Saunders et al., 2018). In this paper, saturation is defined as a cross-sector replication of key codes, not a predetermined number of interviews.

Thematic analysis approach of Braun and Clarke (2022) and Application of ATLAS.ti software (Frieze, 2023) have been applied to systematically identify patterns, codes and categorization which will later be used for proposing the Cyber Trust model. The feedback received while developing the model was used to support the findings and then the I-CVI/S-CVI results of the model were obtained from an independent four-member expert panel, which are reported in the Model Validation section below.

The methodological approach is to systematically follow the principles of qualitative research (Braun & Clarke, 2022; Polit & Beck, 2006; Lincoln & Guba, 1985; Creswell & Poth, 2018) to ensure that the study is contributing to the field of cyber and digital trust studies, given the context of digital engagement and digital trust as a critical determinant of successful digital engagement in Malaysia's digital economy.

CONCEPTS, DEFINITIONS, AND LINKS

The semi-structured interviews were analysed using thematic analysis, which provided in-depth understanding of the Malaysian cybersecurity practitioners' understanding of cybersecurity, digital trust and conditions for a safe and secure digital business environment. For data coding and categorization, the process of familiarization, coding, developing categories and refining themes were conducted using ATLAS.ti software based on Braun and Clarke's (2022) and Frieze's (2023) six phases. According to the analysis, the concept of cyber trust is multidimensional, and not only technical security controls, but also the organizational and governance factors influence this, along with the human factors. Each initial code was further subsumed in a sub theme, which was then further included in one of the main themes; for example, the initial code 'phishing' was further subsumed in the sub theme 'Phishing' and then further included in 'Cybersecurity Issues' which in turn forms part of the main theme 'Cyber Trust Challenges'. The same progression of initial code, sub theme, and main theme was followed for each research question and the themes and codes are summarized in Table 1.

Table 1: Coding framework derived from ATLAS.ti thematic analysis

Research Question	Main Theme	Codes / Sub-Themes
RQ1: Cyber Trust Challenges	Cybersecurity Issues	Data breaches, digital payment fraud, hackers, malware attacks, and network vulnerabilities. Phishing, Ransomware
	Trust-Specific Issues	Data fraud, difficulty authenticating, and financial loss. Gain digital trust; Identity theft; Irresponsible user behaviour; Lack of awareness: Managing sensitive data
RQ2: Cyber Trust Factors	Digital Security and Governance	Convenience; Government involvement; Operational efficiency; Malware-attack prevention
	Data Protection	Data ethics: Protect business continuity. Protect digital systems: Protecting valuable information
	Secured Digital System	Digital security technologies; Layered defence approach; Secured system pillars
RQ3: Technological Elements to Mitigate Challenges	Technological Mitigation	Applying authentication system; Blockchain technology adoption; Centralized system platform; Strict security controls
RQ4: Digital Trust Framework	Awareness	Education and awareness: Security awareness
	Acts, Policies and Governance	Government digital act; Physical security actions; safety procedures, and security policies
	Layered Cybersecurity Framework	Layered cybersecurity framework

The four dimensions of cyber trust related to the digital economy in Malaysia emerged from the analysis of participants' accounts of digital trust, these being the following: Cybersecurity Challenges, Governance and Organizational Competence, Technology Security Measures, and Digital Trust Antecedents. The sum of these dimensions would create the proposed Cyber Trust Model (as shown in Figure 1).

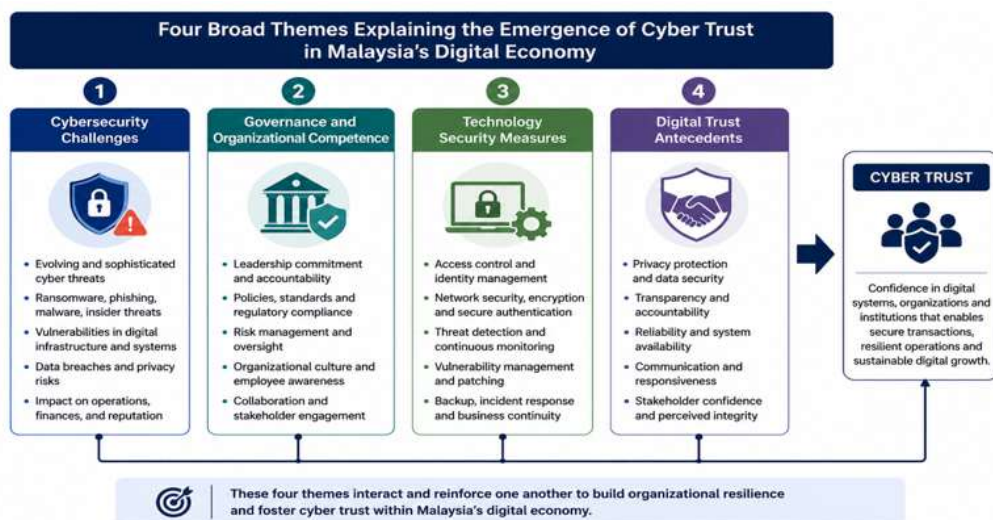


Figure 1. Four broad themes explaining the emergence of cyber trust in Malaysia's digital economy.

Fig. 1: Four broad themes explaining the emergence of cyber trust in Malaysia's digital economy

Cybersecurity Challenges within Malaysia's Digital Economy

As cybersecurity continues to be a major issue for organisations in Malaysia, practitioners are able to identify a number of threats, such as ransomware, malware, phishing, data breaches, unauthorised access and, more recently, fraud associated with the proliferation of digital payments. The dangers have become more complex and more pervasive with the increasingly widespread use of digital technologies in organizations. This is similar to previous reports that highlight cyberattacks as a growing and ongoing threat, which are expected to grow further in the future as technology continues to evolve (World Economic Forum [WEF] 2024; National Institute of Standards and Technology [NIST] 2024; IBM Security, 2024). As one practitioner with over three decades of experience in digital identity and cybersecurity put it, "Malware is the top risk globally, and users should know that they should NOT click on links," while another, whose organisation delivers managed cybersecurity services, described the encryption stage of a ransomware attack as producing "catastrophic" consequences once triggered.

This study builds on the previous work by identifying that technical threats are not the only ones that contribute to the loss of trust in digital systems. Instead, the results indicate that the consequences of cybersecurity incidents, especially those related to trust, significantly amplify the effects of these events on incidents, such as identity theft, authentication failures, financial loss, reputational damage, limited situational awareness, and concerns about how sensitive information is handled.

Most importantly, cyber threats have a significant impact on informational assets and trust in digital relationships. One of the participants said, "Trust is a glass vase, it's a lot easier to break than it is to put it back together again." This description highlights the interdependency between digital security and trust: protecting digital systems and building stakeholder trust is a single goal in practice (Mayer et al., 1995; OECD 2024; Confente et al., 2023). A public-sector participant offered a similarly direct formulation, describing cybersecurity as "the bedrock of digital trust" in the digital services her institution delivers to citizens.

Digital Trust Factors Identified Through Interviews (RQ2)

Users will be more inclined to trust digital systems if they have effective governance and safety frameworks, as this would increase the visibility of their security and decrease uncertainty. Several factors can alleviate such uncertainty and enhance the trust that users have in digital systems, such as government regulation, cybersecurity laws and organizational policy (OECD, 2024; Dhillon et al., 2021). Practitioners linked this directly to recent legislation: one regulatory-sector participant pointed to the Online Safety Act 2025 as a direct governance response to the digital harms she encounters in her role, while another argued more generally for "heavy penalties" and "strengthening laws" as preconditions for deterring cybercrime.

Protection of personal information was identified as another important factor that influenced trust. When users share personal information, they expect the organization to keep the information confidential and when these organizations are visibly showing good ethics in handling the data, it is more likely that they will be trusted. This result aligns with previous studies that have shown that data privacy protection is a key aspect of trust in digital environments (Confente et al., 2023; Gefen et al., 2003; McKnight et al., 2011). One participant described data protection as "vital for safeguarding business continuity and maintaining customer trust," framing it as a business-continuity issue as much as a compliance obligation.

The participants also highlighted the significance of a secure technological infrastructure, as they believed that the trust level is enhanced by transparent security protocols like encryption features, authentication processes, robust infrastructure, and multi-layered security approaches. This highlights the

importance of technology safeguards as a way to instill user and stakeholder confidence (NIST, 2024; ISO/IEC, 2022). All these results suggest that digital trust is not created by a single isolated security control, but rather by the interplay between governance, data protection and technological security control. This was illustrated concretely by two contrasting accounts: one participant's organisation had deployed Zero Trust Architecture, Multi-Factor Authentication and Next-Generation Firewalls, while another described a more foundational public-sector baseline built on SSL technology and disciplined patch management, together illustrating a resourcing gradient in technological sophistication across Malaysia's digital economy.

Technological Elements Required for Cyber Trust Development

The analysis revealed four technological components that are essential for digital trust: authentication, blockchain technology, centralized digital platforms, and the security measures adopted. Participants identified multi-factor authentication, biometrics, digital certificates, public key infrastructure (PKI), and identity verification as key elements of authentication systems, as they have been consistently discussed in the literature on cybersecurity as one of the most effective ways to prevent unauthorized access and identity-related cybercrime (NIST, 2024). One participant, who helped build Malaysia's early public-key infrastructure, argued that PKI-based digital-identity solutions remain "under-utilised" relative to their proven reliability, even as Multi-Factor Authentication has become a broadly adopted, increasingly routine requirement.

Blockchain technology was also seen as a device for fostering trust, because of its transparency, traceability and immutability. Although blockchain was recognized as a useful technology to improve trust in digital transactions, it was acknowledged that regulation is also a critical challenge (Casino et al., 2019; Zheng et al., 2018). The importance of digital platforms for supporting governance, monitoring, interoperability and standardization, and the reduction of fragmentation in security management, was also noted, as it promotes transparency and accountability in the process. Lastly, participants agreed that strict security measures, such as encryption, access control, audit trails, logging systems, and vulnerability management, are essential for ensuring the security of digital systems, working collaboratively to protect their integrity, confidentiality, and availability (ISO/IEC, 2022; NIST, 2024). One participant with direct experience building Malaysia's early digital-identity infrastructure captured this tension precisely: blockchain is "proven for storing value," he explained, but "there is no legal binding yet for blockchain" in Malaysia. Participants characterised this as a timing problem rather than a design flaw: blockchain's decentralised, disintermediated architecture is technically mature, but Malaysia's regulatory instruments, including the Cyber Security Act 2024 and existing digital-signature legislation, are built around identifiable, centrally accountable intermediaries. The practical path forward participants pointed to was phased regulatory recognition of blockchain-based transactions, with legal status treated as a gating condition for what blockchain can be used for, rather than a judgement on its technical readiness.

All these findings indicate that technology serves as more than just a security tool; it actively promotes trust: technological security features offer tangible proof of an organization's dedication to maintaining digital assets and transactions.

Digital Trust Antecedents

The model brings together four interrelated dimensions that shape trust in digital systems: Cybersecurity Challenges, Digital Trust Factors, Technological Elements, and Framework Enablers.

Together, these dimensions give rise to five constituent forms of trust, shown in Figure 2: Governance Trust (leadership, oversight, policy and ethical governance), Technological Trust (secure technologies, access control, data protection and reliability), Organizational Trust (culture, risk management, internal controls and business continuity), Human Trust (education, ethical behaviour and user responsibility), and Resilience Trust (incident preparedness, detection and response, and continuous improvement). How these five forms of trust interact directly determines the confidence stakeholders place in digital interactions, transactions and relationships, which this study terms digital trust (Mayer et al., 1995; Dhillon et al., 2021; OECD, 2024; Confente et al., 2023).

DEVELOPMENT OF THE CYBER TRUST MODEL

This study leads to the creation of a Cyber Trust Model, which explores the complex relationships between cybersecurity capabilities and trust in the digital world, specifically in Malaysia's online economy. The model views cyber trust as a skill that organizations can develop, and it's made up of four connected parts (Mayer et al., 1995; Organisation for Economic Co-operation and Development [OECD], 2024).

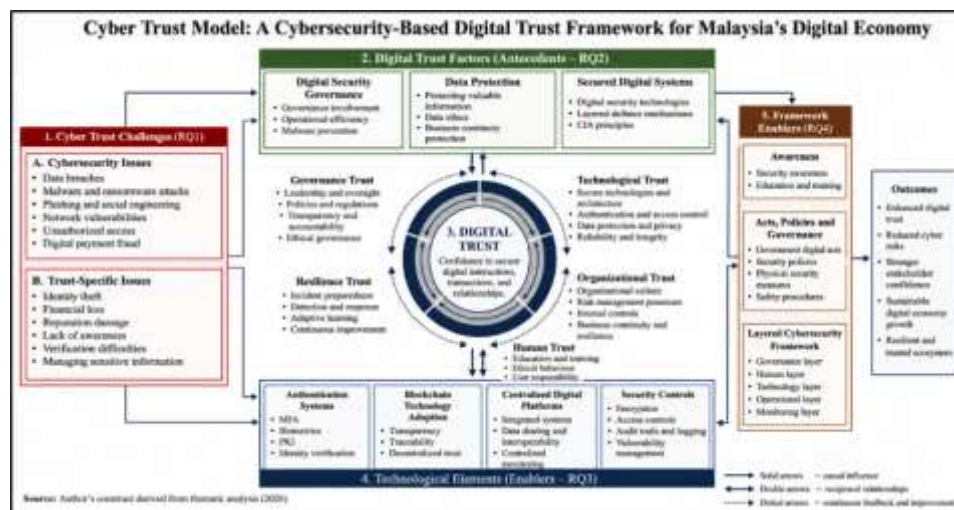


Fig. 2: Cyber Trust Model

There are multiple and interconnected risks to digital enterprises, including external risks that include cyberattacks as well as internal vulnerabilities. The complexity of technology and the constant evolution of threats continue to drive the need for robust cybersecurity solutions, which this study describes as Cybersecurity Challenges.

These challenges also need to be met with good leadership and organizational commitment, which is reflected in Governance and Organizational Competence. This dimension relates to developing a culture of cybersecurity within the organization, compliance with regulations, clarity and adherence to policies, and strategic risk management to support the organization's implementation of cybersecurity strategy (Dhillon et al., 2021; Alshaikh et al., 2022; ISO/IEC, 2022).

Technology Security Measures is the third dimension, which covers the technical protections an organisation can use to safeguard digital assets, such as access control, encryption, network security, vulnerability management, incident response, AI-powered protection, and business continuity planning. All of these mechanisms form the operational framework to protect digital assets and ensure their availability (NIST, 2024; National Institute of Standards and Technology, 2020; ISO/IEC, 2022).

This study's Digital Trust Antecedents are the conditions under which effective cybersecurity practice translates into stakeholder trust as a result of the interaction between these three dimensions. Organizations that are successful in their cybersecurity efforts report that they have increased stakeholder trust in privacy protection, feel they are more transparent and accountable to stakeholder, and communicate and collaborate better. Such results help to build the organization's brand and promote greater engagement with the digital economy. As Figure 2 illustrates, these relationships operate through three distinct kinds of linkage: solid arrows denote a direct causal influence from one construct to another, double arrows denote a reciprocal relationship in which two constructs mutually reinforce one another, and dotted arrows denote a continuous feedback loop, most notably between the five trust dimensions surrounding Digital Trust and the Framework Enablers at the model's periphery, through which improvements in awareness, policy and layered cybersecurity practice feed back into, and are in turn reinforced by, the central trust outcome over time.

Together these four dimensions make the proposed Cyber Trust Model different from the classic cybersecurity models, that mostly focus on technology and compliance separately. Rather, cyber trust is achieved through interactions among governance, technology, human behavior, and relationships among stakeholders, which are interdependent and influence the resilience of digital organizations to sustain their secure digital transformation. This is aligned with what has been proposed in the previous studies (Dhillon et al., 2021; Alshaikh et al., 2022; Vial, 2019).

The model underscores the importance of protecting cybersecurity while fostering trust among stakeholders in increasingly complex digital worlds and is grounded in experiences of cybersecurity practitioners, providing both theoretical and practical value for the organization. It does so by offering a holistic framework that connects governance, technology, organisational capacity and trust, and one directly applicable to policymakers, organisational leaders and cybersecurity practitioners seeking to help Malaysia achieve sustainable digital transformation.

MODEL VALIDATION: CONTENT VALIDITY INDEX RESULTS

Following model development, content validity was assessed by an independent four-member expert panel spanning academic, government-linked research, national digital-policy and national cybersecurity-authority perspectives. Each expert rated 36 items across five evaluation criteria, Relevance, Completeness, Practicality, Applicability and Overall Evaluation, using a five-point scale, following the calculation procedure set out by Polit and Beck (2006) and Yusoff (2019). These five criteria evaluate the model as a whole rather than scoring each of the four content dimensions (Cybersecurity Challenges, Governance and Organizational Competence, Technology Security Measures, and Digital Trust Antecedents) separately; a dimension-level breakdown is identified below as a direction for future validation work.

Table 2: Content validity index results by evaluation criterion (N = 4 Experts, 36 Items)

Criterion	Items	S-CVI/Ave	Mean Score (1–5)	Interpretation
A. Relevance	8	1.000	4.75	Excellent
B. Completeness	8	1.000	4.59	Excellent

<https://doi.org/10.24191/140tsf68>

C. Practicality	8	0.938	4.56	Excellent
D. Applicability	8	0.969	4.75	Excellent
E. Overall Evaluation	4	1.000	4.81	Excellent
Overall (36 items)	36	0.979	4.68	Excellent

The overall Scale-level Content Validity Index across all thirty-six items and four experts was 0.979, with a grand mean rating of 4.68 out of 5.00, both within the “Excellent” band ($S\text{-CVI}/Ave \geq 0.90$) and comfortably above the ≥ 0.78 minimum threshold conventionally applied to expert panels of three to five members. Item-level scores fell below ceiling only on three items, all concerning the model's practicality and applicability for small and medium-sized enterprises specifically, which the expert panel's qualitative feedback linked to a need for simplified, resource-sensitive implementation guidance rather than to any structural weakness in the four-dimension model itself.

DISCUSSION

The Cyber Trust Model proposed here differs from established cybersecurity frameworks such as the NIST Cybersecurity Framework 2.0 and ISO/IEC 27001 in that those frameworks organise practice primarily around technical controls, risk management processes and compliance obligations, treating trust, where it appears at all, as an implicit downstream consequence of adequate security rather than as an explicit, separately theorised construct (NIST, 2024; International Organization for Standardization, 2022). The model also differs from established digital-trust theory: McKnight et al.'s (2002) trust-formation typology and Gefen et al.'s (2003) integration of trust with technology acceptance were built to explain an individual user's one-off decision to trust a website or vendor, and centre on perceived vendor benevolence, ability and integrity. By contrast, the Cyber Trust Model developed here treats digital trust as an organisational-level, socio-technical capability that emerges from the sustained interaction of governance, technology, human behaviour and resilience, consistent with, and extending, the institutional and socio-technical trust literature (Mayer et al., 1995; Bostrom & Heinen, 1977; Dhillon et al., 2021). This reframing is the study's principal theoretical contribution: it repositions digital trust from an outcome that follows automatically from good security practice to a structural design objective that organisations must deliberately build across four distinct but interdependent dimensions.

Several limitations qualify these findings. The study is based on ten semi-structured interviews across three sectors, an appropriate sample for exploratory, theory-building qualitative research but one that limits statistical generalisability to the wider population of Malaysian digital businesses; readers should treat the model as an empirically grounded framework for further testing rather than as a population-level claim (Myers, 2020; Eisenhardt & Graebner, 2007). The study is also confined to the Malaysian regulatory and institutional context, so the specific weighting of the model's dimensions, particularly Governance and Organizational Competence, which is closely tied to Malaysia-specific instruments such as the Cyber Security Act 2024, may not transfer directly to other jurisdictions without adaptation. Data collection was cross-sectional, capturing practitioners' accounts at a single point in time rather than tracking how digital trust develops or erodes over the course of an incident or a regulatory change. Finally, while the four-member expert panel's Content Validity Index results were strong (overall $S\text{-CVI}/Ave = 0.979$), a larger and more diverse panel, and a dimension-level rather than criterion-level validation exercise, would strengthen confidence in the model's structure still further.

Building on these limitations, three directions for future research follow directly from this study's findings. First, the qualitative model developed here could be operationalised as a survey instrument and tested quantitatively, for example using Partial Least Squares Structural Equation Modelling, an approach

already applied successfully to related technology-adoption questions in the Malaysian context (Rahim et al., 2022), to test the strength and direction of the relationships between the model's four dimensions and organisational trust outcomes at scale. Second, the model's content validity would benefit from a dimension-level validation exercise, ideally with a larger and sector-balanced expert panel, that scores each of the four dimensions independently rather than the model as a whole. Third, cross-country replication, particularly within other ASEAN digital economies navigating comparable regulatory modernisation, would help establish which elements of the model are Malaysia-specific and which reflect more general patterns in the relationship between cybersecurity practice and digital trust.

CONCLUSION

The aim of this study was to explore the issues affecting organisations and individuals in keeping people safe online; what makes online environments trustworthy; how technology can facilitate that trust; and the needs for building a coherent trust framework in Malaysia's digital economy. It surveyed key challenges to digital trust and factors that impact digital trust, as discovered in interviews with cybersecurity practitioners, government officials, IT practitioners, and digital business leaders. The results have shown that security technology is not enough to create trust in digital systems, but the trust is built with the presence of effective governance, organizational capabilities, trustworthy behavior, technological security, and systemic resilience.

This study builds on these findings and introduces the Cyber Trust Model as a way to understand the development and maintenance of digital trust. The model provides a framework for a more structured approach to establishing trust, security, and resilience within the country's digital economy in the face of digital transformation's rapid pace, offering a shared foundation for organizations, policymakers, and researchers alike to enhance the safety and trustworthiness of Malaysia's digital economy. Finally, the study illustrates that cybersecurity is not just about protection, rather it is about being trusted, it is about the basis for sustainable digital transformation and it is about growth in the long-term in the digital economy. With proper application, the proposed model can be a roadmap to achieving digital society that is secure, trusted and resilient.

THEORETICAL IMPLICATIONS

This study contributes to the existing body of knowledge in several ways. First, it extends cybersecurity literature by introducing trust as a central analytical construct rather than a secondary outcome. Second, it brings together institutional trust theory, socio-technical systems theory, and cybersecurity governance perspectives into a unified conceptual framework. Third, the Cyber Trust Model provides an empirically grounded framework developed specifically within the Malaysian digital economy context. Fourth, the study demonstrates that digital trust is multidimensional and influenced by governance, technology, organizational culture, human behavior, and resilience capabilities.

PRACTICAL AND MANAGERIAL IMPLICATIONS

Beyond its theoretical contribution, the Cyber Trust Model offers concrete guidance for Chief Information Security Officers (CISOs), organisational leaders and policymakers. For CISOs, the model's central implication is that technical investment alone is insufficient: because Cybersecurity Issues in this study were most consistently attributed to lack of awareness and irresponsible user behaviour rather than attacker sophistication, organisations, particularly smaller and resource-constrained ones, are likely to see a better return from structured staff awareness programmes than from further layering technical controls

onto an already under-used base. The Human Firewall principle articulated by participants, that well-trained users function as an active line of defence rather than a passive vulnerability, offers CISOs a practical framing for justifying awareness investment to organisational leadership in the same terms as technical spending. The finding that authentication technologies, encryption, and layered, multi-domain security approaches recurred independently across practitioners from unrelated organisations further suggests that CISOs adopting a similarly layered Administrative-Technical-Physical-Legal structure will be aligning with what already functions as a de facto professional standard in Malaysia's digital economy, rather than introducing an unfamiliar model. For organisational leaders, the model's Governance and Organizational Competence dimension implies that digital trust cannot be delegated to the IT function alone; leadership commitment, regulatory compliance and organisational culture were identified by participants as trust-relevant in their own right, independent of technical capability. For policymakers and regulators, the finding that blockchain adoption in Malaysia is technically mature but legally unrecognised suggests a concrete, actionable policy gap: phased regulatory recognition of blockchain-based transactions would allow Malaysian digital businesses to convert an already-proven technology into a trust-building asset. Finally, because Practicality and Applicability were the two evaluation criteria on which the expert panel's ratings, while still in the "Excellent" band, were comparatively lowest, and because this was linked specifically to small and medium-sized enterprises, policymakers and industry bodies such as MDEC are encouraged to pair the model with simplified, SME-specific implementation guidance, such as a prioritisation checklist or quick-start version of the four dimensions, so that the model's benefits are not confined to larger, better-resourced organisations.

ACKNOWLEDGEMENTS

I want to sincerely thank Universiti Teknologi MARA (UiTM), Puncak Perdana Campus, Selangor, for offering the resources and assistance required for this study. This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors."

CONFLICT OF INTEREST STATEMENT

The authors declare that there is no conflict of interest associated with this research or its publication. The authors confirm that the research was conducted without any commercial, financial, or personal interests that could have influenced the work.

AUTHORS' CONTRIBUTIONS

Amuhaimi: Conceptualization, Investigation, Data Curation, Formal Analysis, Writing – Original Draft, Writing – Review & Editing.

Khairulnizam: Subject Matter Expertise, Conceptualization, Writing – Original Draft, Writing – Review & Editing, Validation.

Irni: Methodology, Formal Analysis, Validation, Writing – Review & Editing.

All authors contributed to the development and refinement of the manuscript, reviewed the final version, and approved the manuscript for submission.

REFERENCES

- Alshaikh, M., Maynard, S. B., Ahmad, A., & Chang, S. (2022). Understanding cybersecurity culture and governance: A systematic literature review. *Computers & Security*, 113, 102551. <https://doi.org/10.1016/j.cose.2021.102551>
- Bada, M., Sasse, A. M., & Nurse, J. R. C. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? *arXiv*. <https://doi.org/10.48550/arXiv.1901.02672>
- Bostrom, R. P., & Heinen, J. S. (1977). MIS problems and failures: A socio-technical perspective. *MIS Quarterly*, 1(3), 17–32. <https://doi.org/10.2307/248710>
- Braun, V., & Clarke, V. (2022). *Thematic analysis: A practical guide*. SAGE Publications.
- Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Current status, classification and open issues. *Telematics and Informatics*, 36, 55–81. <https://doi.org/10.1016/j.tele.2018.11.006>
- Confente, I., Siciliano, G. G., Gaudenzi, B., & Eickhoff, M. (2023). Digital trust and consumer behavior in the digital economy: A systematic literature review. *Journal of Business Research*, 157, 113584. <https://doi.org/10.1016/j.jbusres.2022.113584>
- Creswell, J. W., & Poth, C. N. (2018). *Qualitative inquiry and research design: Choosing among five approaches* (4th ed.). SAGE Publications.
- CyberSecurity Malaysia. (2024). *Cyber security outlook 2024*. CyberSecurity Malaysia.
- Deloitte. (2023). *Digital trust: The foundation of customer relationships*. Deloitte Insights.
- Dhillon, G., Syed, R., & de Sá-Soares, F. (2021). Information security concerns in information systems research: An agenda for future research. *Information Systems Journal*, 31(3), 513–552. <https://doi.org/10.1111/isj.12367>
- Economic Planning Unit. (2021). *Twelfth Malaysia Plan, 2021–2025*. Prime Minister's Department, Malaysia.
- Eisenhardt, K. M., & Graebner, M. E. (2007). Theory building from cases: Opportunities and challenges. *Academy of Management Journal*, 50(1), 25–32. <https://doi.org/10.5465/amj.2007.24160888>
- Friese, S. (2023). *Qualitative data analysis with ATLAS.ti* (5th ed.). SAGE Publications.
- Gefen, D., Karahanna, E., & Straub, D. W. (2003). Trust and TAM in online shopping: An integrated model. *MIS Quarterly*, 27(1), 51–90. <https://doi.org/10.2307/30036519>
- IBM Security. (2024). *Cost of a data breach report 2024*. IBM Corporation.

- International Organization for Standardization. (2022). ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection—Information security management systems—Requirements. ISO.
- Kallio, H., Pietilä, A.-M., Johnson, M., & Kangasniemi, M. (2016). Systematic methodological review: Developing a framework for a qualitative semi-structured interview guide. *Journal of Advanced Nursing*, 72(12), 2954–2965. <https://doi.org/10.1111/jan.13031>
- Lincoln, Y. S., & Guba, E. G. (1985). *Naturalistic inquiry*. SAGE Publications.
- Malaysia Digital Economy Corporation. (2021). *Malaysia Digital Economy Blueprint (MyDIGITAL)*.
- Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *Academy of Management Review*, 20(3), 709–734. <https://doi.org/10.2307/258792>
- McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and validating trust measures for e-commerce: An integrative typology. *Information Systems Research*, 13(3), 334–359. <https://doi.org/10.1287/isre.13.3.334.81>
- Myers, M. D. (2020). *Qualitative research in business and management* (3rd ed.). SAGE Publications.
- National Institute of Standards and Technology. (2020). *Zero Trust Architecture* (Special Publication 800-207). U.S. Department of Commerce.
- National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0*. U.S. Department of Commerce.
- Organisation for Economic Co-operation and Development. (2024). *Building digital trust for a resilient digital economy*. OECD Publishing.
- Patton, M. Q. (2015). *Qualitative research & evaluation methods* (4th ed.). SAGE Publications.
- Polit, D. F., & Beck, C. T. (2006). The Content Validity Index: Are you sure you know what's being reported? Critique and recommendations. *Research in Nursing & Health*, 29(5), 489–497. <https://doi.org/10.1002/nur.20147>
- Ponemon Institute. (2024). *Cost of cyber crime study 2024*. Ponemon Institute.
- Rahim, N. A., et al. (2022). AI-based chatbots adoption model for higher-education institutions: A hybrid PLS-SEM-neural network modelling approach. *Sustainability*, 14(19), 12726.
- Saunders, B., Sim, J., Kingstone, T., Baker, S., Waterfield, J., Bartlam, B., Burroughs, H., & Jinks, C. (2018). Saturation in qualitative research: Exploring its conceptualization and operationalization. *Quality & Quantity*, 52(4), 1893–1907. <https://doi.org/10.1007/s11135-017-0574-8>

- Siponen, M., & Vance, A. (2010). Neutralization: New insights into the problem of employee information systems security policy violations. *MIS Quarterly*, 34(3), 487–502.
- Taherdoost, H. (2022). Understanding cybersecurity frameworks and information security standards: A review. *Information*, 13(9), 430. <https://doi.org/10.3390/info13090430>
- United Nations. (2024). United Nations E-Government Survey 2024: Accelerating digital transformation for sustainable development. United Nations.
- 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>
- Verhoef, P. C., Broekhuizen, T., Bart, Y., Bhattacharya, A., Dong, J. Q., Fabian, N., & Haenlein, M. (2021). Digital transformation: A multidisciplinary reflection and research agenda. *Journal of Business Research*, 122, 889–901. <https://doi.org/10.1016/j.jbusres.2019.09.022>
- Vial, G. (2019). Understanding digital transformation: A review and a research agenda. *The Journal of Strategic Information Systems*, 28(2), 118–144. <https://doi.org/10.1016/j.jsis.2019.01.003>
- von Solms, R., & van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, 38, 97–102. <https://doi.org/10.1016/j.cose.2013.04.004>
- Whetten, D. A. (1989). What constitutes a theoretical contribution? *Academy of Management Review*, 14(4), 490–495. <https://doi.org/10.5465/amr.1989.4308371>
- World Bank. (2021). World Development Report 2021: Data for better lives. World Bank. <https://doi.org/10.1596/978-1-4648-1600-0>
- World Economic Forum. (2024). Global Cybersecurity Outlook 2024. World Economic Forum.
- Yusoff, M. S. B. (2019). ABC of Content Validation and Content Validity Index calculation. *Education in Medicine Journal*, 11(2), 49–54. <https://doi.org/10.21315/eimj2019.11.2.6>
- Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: A survey. *International Journal of Web and Grid Services*, 14(4), 352–375. <https://doi.org/10.1504/IJWGS.2018.095647>



© 2026 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).