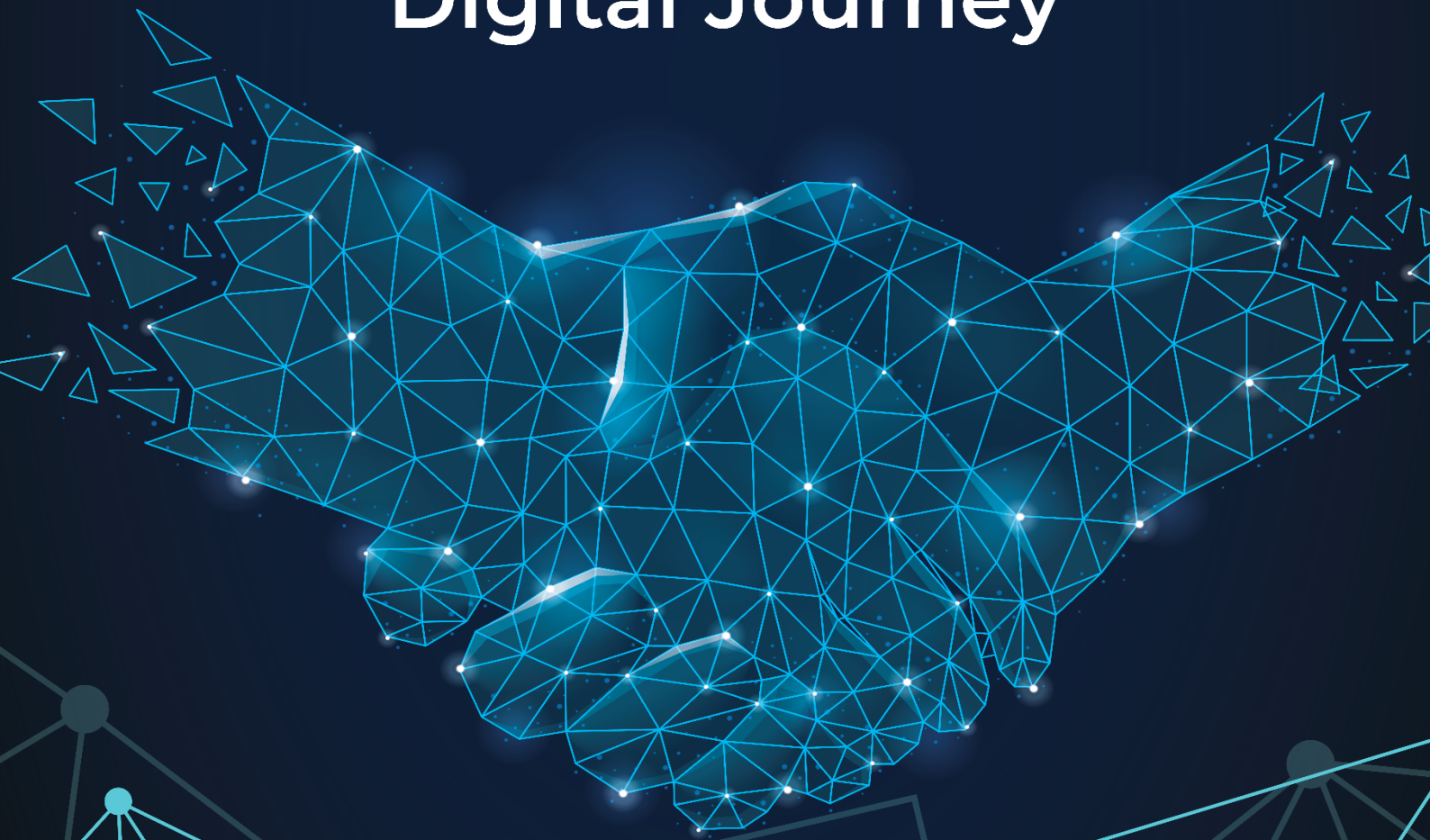
MINISTRY OF DIGITAL

CyberSecurity MALAYSIA

Securing Tomorrow: Building Trust in Malaysia's Digital Journey



April 2025

Contents

EXECUTIVE SUMMARY

In an era of rapid digital transformation, **digital trust** has emerged as a cornerstone of Malaysia's journey toward a resilient and inclusive digital economy. Trust in digital technologies, systems, and services is not merely a technical necessity but a strategic imperative that underpins economic growth, social cohesion, and national security. As Malaysia embraces initiatives like the **National Digital Economy Blueprint**, establishing a robust digital trust framework is essential to enhance public confidence in e-governance, drive secure online transactions, and empower citizens in their digital interactions.

This document outlines Malaysia's vision for building a **trusted digital ecosystem**, where individuals, businesses, and government entities can interact securely and confidently. By prioritising user safety, promoting ethical technology use, and ensuring access to reliable digital services, Malaysia aims to position itself as a regional leader in the digital economy. Achieving this vision requires a **holistic approach** that integrates **cybersecurity**, **data protection**, **transparency**, and **public engagement** into a cohesive national framework.

Key Insights and Strategic Recommendations

Strengthening Cybersecurity

Implement stringent cybersecurity protocols, including a **zero-trust security model**, to protect sensitive data and enhance consumer confidence. Proactive measures are essential to mitigate risks and build resilience against evolving cyber threats.

Enhancing Data Protection

Develop robust data protection strategies that align with international standards, such as the **General Data Protection Regulation (GDPR)**, to safeguard user information and foster trust. Compliance with regulations like the **Personal Data Protection Act (PDPA)** is critical for ensuring accountability and transparency.

Promoting Transparency

Increase clarity around data collection, usage, and protection practices to mitigate negative perceptions and improve user confidence. Transparent communication is key to building trust in digital services.

International Collaboration

Foster global partnerships to share best practices, resources, and knowledge in combating cyber threats. Aligning with international standards will enhance Malaysia's competitiveness and credibility in the global digital economy

Cultivating a Digital Trust Culture

Engage the public in discussions about cybersecurity and data protection through education and awareness initiatives. A well-informed citizenry is essential for fostering a culture of trust and responsible digital behaviour.

Vision for a Trusted Digital Ecosystem

Malaysia's vision is to create a digital ecosystem where all stakeholders—government, businesses, and citizens—can interact securely and confidently. This ecosystem will prioritize **user safety**, **ethical technology use**, and **reliable digital services**, ensuring that the benefits of digital transformation are accessible to all. By fostering a culture of digital trust, Malaysia aims to unlock the full potential of its digital economy, driving innovation, investment, and inclusive growth.

Next Steps: National Digital Trust Framework and National Digital Trust Centre

To realize this vision, Malaysia must establish a **National Digital Trust Framework** that integrates cybersecurity measures, data protection standards, transparency protocols, and public engagement strategies. Additionally, the creation of a **National Digital Trust Centre** will serve as a hub for promoting best practices, facilitating stakeholder collaboration, and enhancing public understanding of digital services. These initiatives will collectively strengthen Malaysia's digital trust landscape, ensuring sustainable growth in the digital age.

In conclusion, building digital trust is not just a technical challenge but a **shared responsibility** that requires the active participation of all stakeholders. By prioritizing cybersecurity, data protection, transparency, and public engagement, Malaysia can create a secure, inclusive, and innovation-driven digital ecosystem that empowers its citizens and positions the nation as a leader in the global digital economy.

INTRODUCTION

In an increasingly interconnected world, **digital trust** has become a foundational pillar for the success of nations, businesses, and individuals. Trust in digital technologies, systems, and services is no longer a luxury but a necessity, as it underpins economic growth, social cohesion, and national security. For Malaysia, a country on a transformative digital journey, fostering digital trust is not just a strategic imperative—it is a **national mission** that will determine the success of its digital economy and the well-being of its citizens.

This document underscores the critical importance of Digital Trust as the foundation of Malaysia's digital future, positioning it as the key enabler of a secure, inclusive, and globally competitive digital ecosystem.

What is Digital Trust?

Digital Trust refers to the confidence that individuals, businesses, and governments place in digital technologies, systems, and services, based on their **security**, **privacy**, **reliability**,and **ethical conduct**. It is built on the foundational principles of **data protection**, **cybersecurity**, **transparency**, and the **responsible use of technology**. Digital Trust is not merely about technical measures; it extends to the **social**, **ethical**, and **legal frameworks** that underpin the digital ecosystem.

In essence, Digital Trust is the assurance that digital interactions—whether between individuals, companies, or government entities—are **safe**, **transparent**, and conducted with **integrity**. It allows users to feel confident that their personal information is protected, that digital platforms operate securely, and that emerging technologies are used responsibly and fairly. Trust is central to the acceptance and adoption of digital innovations, and its absence can undermine technological progress, limit economic growth, and jeopardize public safety.

Why Digital Trust Matters for Malaysia

Digital trust is increasingly recognized as a fundamental pillar for Malaysia's success in the digital age, impacting the government, businesses, and citizens in significant ways. As the nation embraces digital transformation through initiatives like Malaysia 5.0 and the National Digital Economy Blueprint, understanding the implications of digital trust across these three categories is essential.

1. GOVERNMENT

Enhancing Public Confidence: For the government, establishing digital trust is vital to foster public confidence in digital services. As citizens rely more on e-governance and online public services, they need assurance that their personal data is protected from misuse and breaches. A lack of trust can lead to underutilization of these services and potential regulatory setbacks. The government's role in safeguarding data and ensuring transparency is crucial for maintaining this trust, which directly influences citizen engagement with digital initiatives.

Supporting National Security: Additionally, as Malaysia's infrastructure becomes more reliant on digital technologies, the government must prioritize cybersecurity to protect national interests. Strengthening digital trust helps mitigate risks associated with cyber threats, ensuring that sensitive information remains secure against espionage and cybercrime. This proactive approach not only safeguards citizens but also reinforces Malaysia's position in the global arena as a secure destination for investment.

2. BUSINESSES

Driving Economic Growth: For businesses, digital trust is essential for fostering economic growth within the digital economy. Companies depend on consumer confidence to engage in e-commerce and other online transactions. When consumers perceive a lack of trust in digital platforms, it can stifle innovation and deter investment. By prioritizing digital trust, businesses can create a secure environment that encourages online participation and enhances their competitive edge.

Compliance and Reputation: Furthermore, adherence to regulations such as the Cyber Security Act 2024 not only ensures compliance but also builds a reputation for reliability among consumers. Organizations that demonstrate a commitment to protecting user data and maintaining high security standards are more likely to gain customer loyalty and attract new clients. This focus on building trust can serve as a significant competitive advantage in an increasingly crowded marketplace.

3. CITIZENS

Empowering Individuals: For citizens, digital trust translates into empowerment and safety in their daily interactions with technology. As Malaysians engage more with digital banking, e-commerce, and smart city initiatives, they need confidence that their personal information is handled responsibly. Trust in digital services fosters greater participation in the digital economy, ultimately enhancing quality of life through improved access to services and opportunities.

Combating Misinformation: Moreover, a trustworthy digital environment helps combat misinformation and promotes social cohesion. Citizens who feel secure in their online interactions are more likely to engage positively within their communities, contributing to a safer and more harmonious society. This collective engagement is vital for Malaysia's aspirations of becoming a regional leader in the digital economy.

In summary, digital trust is not merely a technical necessity; it is a critical enabler for the government, businesses, and citizens alike. By fostering an environment of trust, Malaysia can fully harness the potential of its digital transformation efforts while ensuring security, privacy, and fairness for all stakeholders.

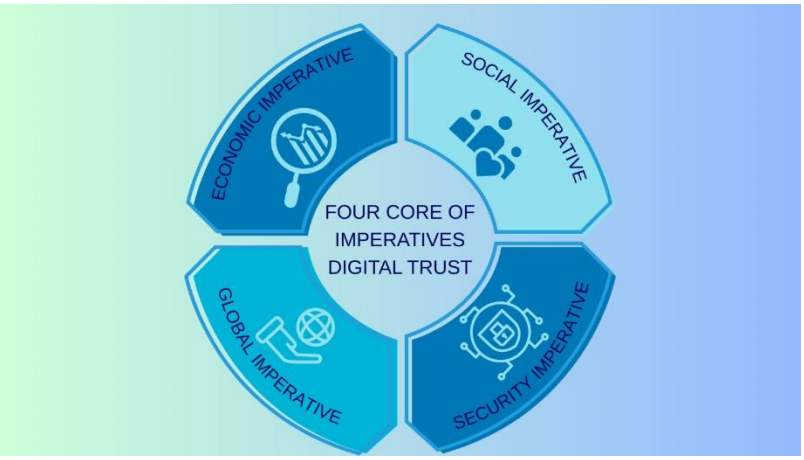


Figure 1: The Four Core of Imperative Digital Trust

The Four Core Imperatives of Digital Trust

To fully understand the importance of digital trust, as illustrated in Figure 1, it is essential to recognize its **four core imperatives**:

1. **Economic Imperative**: Digital trust is a powerful enabler of Malaysia's **economic growth**. It attracts investment, accelerates e-commerce, and fosters innovation by reducing transaction costs and lowering market entry barriers. Businesses flourish when consumers and enterprises trust digital platforms, creating a dynamic ecosystem where entrepreneurship thrives.
2. **Social Imperative**: A trusted digital environment is essential for building an **inclusive society** where all Malaysians—regardless of background—can confidently participate in the digital economy. Secure and transparent digital systems protect consumer rights, promote digital literacy, and ensure that the benefits of digital transformation are shared equitably.
3. **Security Imperative**: As cyber threats grow in scale and complexity, **security** is a cornerstone of digital trust. A strong trust framework safeguards national infrastructure, critical systems, and personal data, ensuring resilience against cyberattacks, fraud, and misinformation. By prioritizing cybersecurity and data protection, Malaysia can enhance the integrity of its digital interactions and strengthen national security.
4. **Global Imperative**: In an interconnected world, **global alignment** in digital trust practices is essential. By adopting international best practices and regulatory frameworks, Malaysia can foster cross-border trade, attract foreign investments, and position itself as a leader in the global digital economy. Trust enables seamless international collaboration, strengthening Malaysia's influence and competitiveness on the world stage.

A Holistic Framework for Digital Trust

Building digital trust is not a one-dimensional challenge; it requires a **holistic framework** that integrates **technological**, **social**, **ethical**, and **legal** dimensions. This framework must prioritize **user safety**, **transparency**, and **ethical technology use**, while also fostering a culture of trust through education and awareness initiatives. By aligning these elements, Malaysia can create a **resilient digital ecosystem** that protects data, promotes innovation, and empowers all stakeholders.

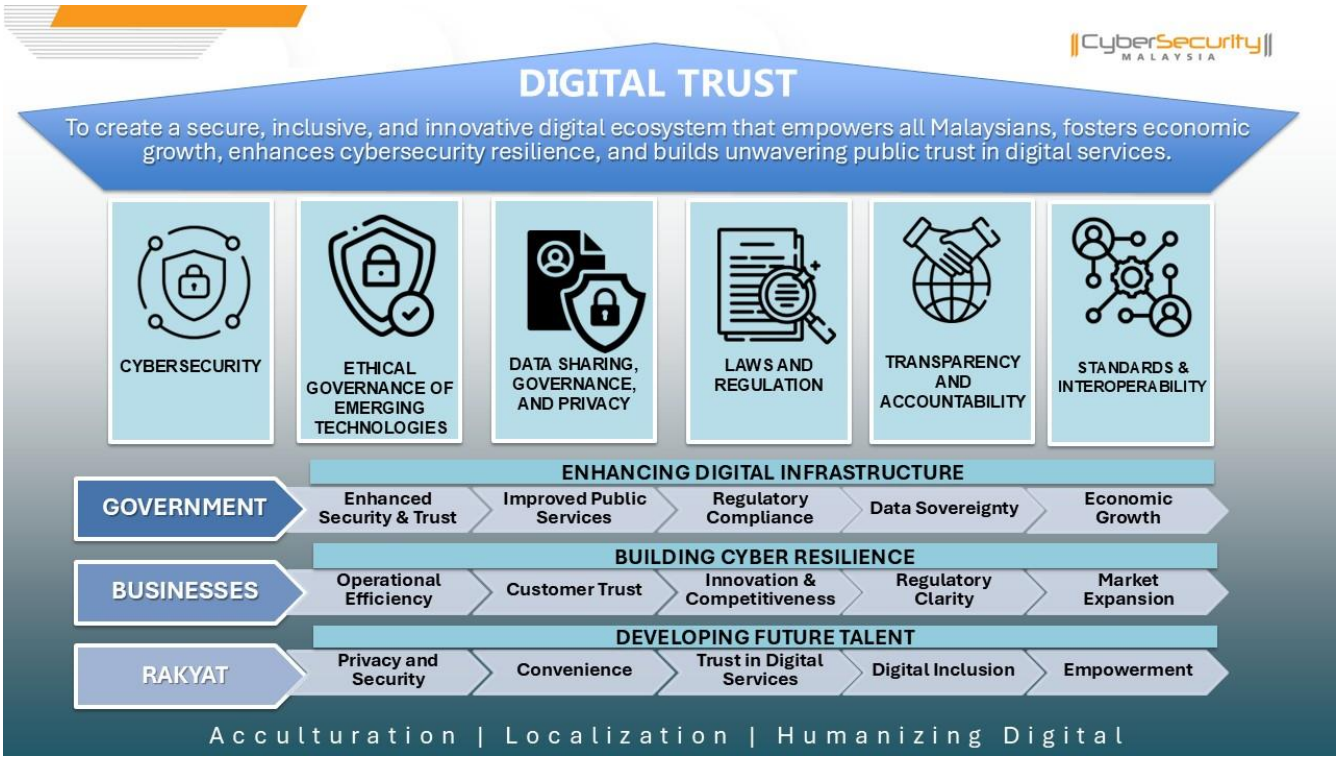


Figure 2: The Digital Trust Framework

The Path Forward

As Malaysia navigates the complexities of the digital age, fostering digital trust will be essential to unlocking the full potential of its digital transformation efforts. This document serves as a **blueprint** for the development of a **National Digital Trust Framework**, providing actionable insights and strategic recommendations for policymakers, businesses, and citizens. By prioritizing digital trust, Malaysia can build a secure, inclusive, and innovation-driven digital ecosystem that positions the nation as a leader in the global digital economy.

Global Context and Digital Trust Landscape

Global Digital Trust Models and Frameworks

In the digital era, trust frameworks have become critical for fostering confidence in digital interactions, transactions, and data exchanges. Across the globe, nations have developed tailored approaches to address their unique challenges and leverage their strengths in building digital trust. These frameworks emphasize **regulatory measures**, **public engagement**, and **technological innovation**, creating a foundation for secure and trustworthy digital economies.

In evaluating the digital trust frameworks across various countries, it is evident that each nation has tailored its approach to address specific challenges and leverage unique strengths.

Collectively, these frameworks illustrate a global trend toward prioritizing digital trust through regulatory measures, public engagement, and technological innovation. Integrating robust legal structures, public-private partnerships, and comprehensive cybersecurity strategies is essential for fostering a secure and trustworthy digital economy. This trend underscores the necessity of adapting digital trust frameworks to local contexts while drawing on successful practices from other nations. Ultimately, the commitment to enhancing digital trust is vital for consumer protection and promoting innovation and economic growth in the digital age.

Key Observations on Digital Trust Frameworks

01

Tailored Approaches

Countries have developed frameworks that address local challenges while leveraging unique strengths. For example, Kenya's Digital Economy Blueprint emphasizes cybersecurity and public awareness, while Saudi Arabia's National Cybersecurity Strategy focuses on stringent legislation against cybercrimes.

02

Compliance and Consumer Protection

Strong compliance standards and consumer protection policies are essential for enhancing trust in digital technologies. Australia's Trusted Digital Identity Framework and South Korea's legal frameworks for electronic transactions exemplify this approach.

03

Integration of Legal and Cybersecurity Strategies

Combining robust legal structures with comprehensive cybersecurity strategies is critical for fostering a secure digital economy. Germany's adherence to GDPR and Canada's Digital Charter highlight the importance of this integration.

04

Public Engagement and Transparency

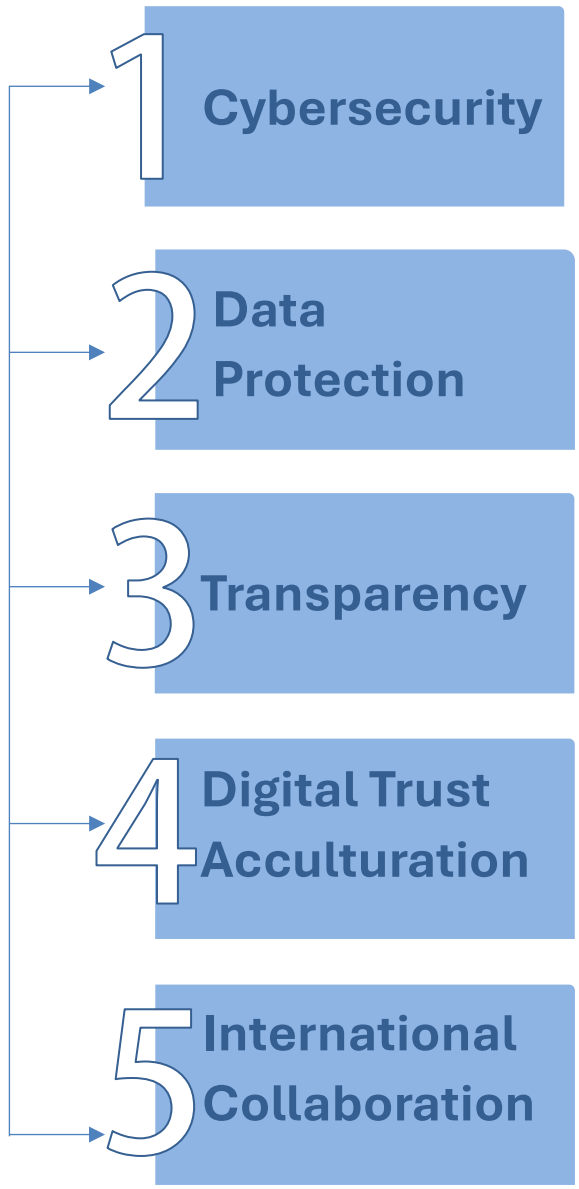
There is a growing recognition of the need for public engagement in digital trust initiatives. Kenya's collaboration with the private sector and Belgium's citizen engagement initiatives demonstrate the value of transparency and accountability.

Lessons for Malaysia

Malaysia can draw valuable insights from these global models to strengthen its digital trust framework. By adopting international best practices, fostering public-private partnerships, and prioritizing transparency, Malaysia can build a resilient digital ecosystem that enhances user confidence and drives economic growth.

KEY COMPONENTS FOR BUILDING A ROBUST DIGITAL TRUST ECOSYSTEM

The global mapping of digital trust frameworks and models identifies essential components, including cybersecurity, data protection, transparency, digital trust acculturation, and international cooperation. Every element is crucial in fostering trust within digital environments, particularly as the reliance on digital technologies increases. These five components are highlighted to ensure that a country's digital trust framework is effective and resilient despite evolving technological challenges



- **Cybersecurity:** Cybersecurity is a cornerstone of digital trust, necessitating the implementation of stringent security protocols to protect sensitive data from cyber threats. Effective cybersecurity measures not only safeguard data but also enhance consumer confidence in online services. The adoption of a zero-trust security model, which continuously validates every interaction, is a vital initiative within the comprehensive framework of cybersecurity aimed at significantly reducing the risk of cyberattacks. This model not only plays a crucial role in protecting digital infrastructures but also complements other strategies designed to bolster security and maintain user trust across various platforms.

- **Data Protection:** Data protection is integral to the digital trust framework. Implementing robust data protection strategies ensures the confidentiality and integrity of user information. Technologies such as blockchain can enhance data security through tamper-proof verification and secure management. Additionally, compliance with regulations like the Personal Data Protection Act in Malaysia as well as the General Data Protection Regulation (GDPR) in Europe demonstrates an organization's commitment to safeguarding personal data, thereby fostering consumer trust.

- **Transparency:** Transparency is vital for building confidence in digital interactions. Providing clear and understandable information regarding data collection, usage, and protection is essential. Enhanced transparency not only improves trust but also mitigates negative perceptions among users. Clarifying compliance standards in digital services and consumer protection measures further strengthens consumer confidence.

- **Digital Trust Acculturation:** Cultivating a culture of digital trust requires public engagement in discussions about cybersecurity and data protection. Educating employees on organizational cybersecurity practices can significantly enhance overall digital trust. Furthermore, involving the public in the development of policies related to digital trust leads to more effective and widely accepted frameworks.

- **International Collaboration:** As cyber threats often cross-national boundaries, international collaboration is increasingly important for enhancing digital trust. Global partnerships facilitate the sharing of best practices and resources to effectively combat cyber threats. Collaborative efforts are essential for establishing standardized cybersecurity and data protection requirements, which are crucial for maintaining trust in the global digital economy. Such cooperation addresses complex cybersecurity challenges within interconnected environments, ensuring secure and confident operations for all stakeholders involved.

Digital Trust in Malaysia: Current State

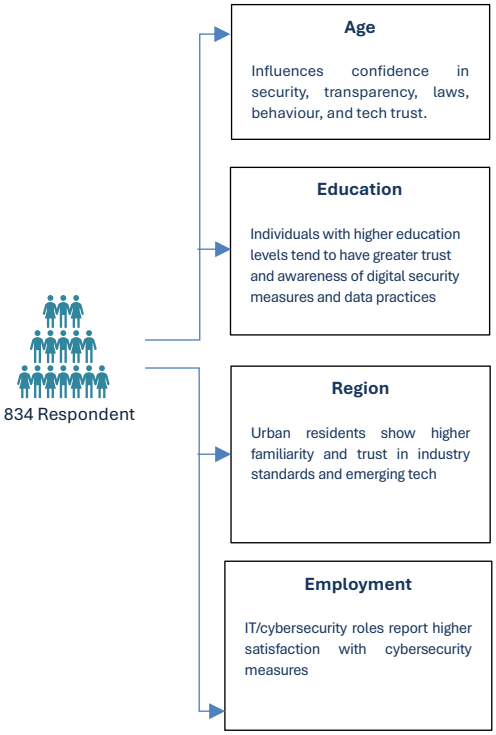
Overview of Malaysia's Digital Trust Landscape

As the digital economy continues to evolve globally, nations are recognizing the importance of establishing digital trust as a cornerstone for sustainable growth. Malaysia too has embarked on several strategic initiatives aimed at fostering digital trust, enhancing cybersecurity, and creating a resilient digital landscape. By leveraging both conventional and digital media, the government has sought to clarify misconceptions and enhance public understanding of digital services, which is crucial for building trust. Additionally, initiatives to promote digital literacy, especially among rural communities, further contribute to a more informed citizenry capable of navigating the digital landscape securely. The section below explores key initiatives in Malaysia that exemplify the country's commitment to building a trustworthy digital economy.

The analysis and investigation of the digital trust landscape in Malaysia reveal critical insights into the current state of digital interactions among citizens, businesses, and government entities. This comprehensive evaluation underscores the significance of trust as a foundational element for fostering a secure and resilient digital economy. By examining various dimensions such as data privacy, cybersecurity measures, and user perceptions, the study identifies both strengths and vulnerabilities within the existing regulatory framework. The findings indicate that while there are robust initiatives in place to enhance digital security, gaps remain that could jeopardize user confidence and hinder the growth of digital services. The deliverables from this investigation provide actionable recommendations aimed at reinforcing digital trust across multiple sectors.

By leveraging stakeholder engagement and promoting transparent communication strategies, stakeholders can cultivate an environment where users feel secure in their online interactions. The emphasis on collaborative efforts among government agencies, private sector players, and civil society is essential for establishing a cohesive approach to enhancing digital trust. This initiative serves as a pivotal step towards not only safeguarding personal data but also promoting innovation and economic development in Malaysia's rapidly evolving digital landscape.

MALAYSIAN DIGITAL TRUST STUDY: FINDINGS FROM PUBLIC & BUSINESS SURVEY



The Malaysian Digital Trust Study, conducted in early 2024, provides a comprehensive overview of how Malaysians perceive digital trust in today's technology-driven landscape. Drawing insights from diverse demographics and sectors, the study aims to identify key factors that influence trust in digital platforms and services. Its objective is to support the development of policies and strategies that foster a secure, inclusive, and trustworthy digital ecosystem in Malaysia.In an era where digital interactions have become integral to daily life and business operations, understanding the nuances of trust in digital environments is crucial. This report draws insights from a robust sample of 834 respondents, facilitating exploration of factors influencing digital trust, including gender, age, education, regional differences, and employment status

In our increasingly digital world, trust is fundamental to users' engagement and satisfaction. The survey's findings provide a foundation for understanding how various demographic factors interplay in shaping digital trust in Malaysia. The survey findings indicate that different age groups in Malaysia show significant relationships with various aspects of digital trust, including confidence in digital security measures, transparency of data collection, satisfaction with cybersecurity measures, stakeholder involvement, effectiveness of laws, familiarity with industry standards, responsible online behaviour, ease of information exchange, and trust in data protection with emerging technologies. Education levels also play a crucial role, significantly influencing confidence in data transparency, satisfaction with cybersecurity, involvement in decision-making, responsible online behaviour, and overall trust in the digital ecosystem. Higher education levels correlate with greater awareness and trust in digital practices and protections. The survey also reveals that the region of residence significantly impacts digital trust, with urban areas showing higher familiarity with industry standards and trust in data protection using emerging technologies. Employment type also affects satisfaction with cybersecurity measures and familiarity with industry standards, particularly for those in IT and cybersecurity roles. However, gender does not significantly influence any of the digital trust factors, suggesting that digital trust is not affected by gender differences. Based on the findings, it could be derived that the Malaysian Digital Trust Framework should consist of **6 major elements, namely, Confidence in Digital Security Measures, Satisfaction with Cybersecurity Measures, Effectiveness of Laws and Regulations, Understanding Responsible Online Behaviour, Ease of Information Exchange, and Confidence in Data Protection with Emerging Technologies**.

INITIATIVES TAKEN BY INDUSTRY KEY PLAYERS OF MALAYSIA IN ENHANCING DIGITAL TRUST

INITIATIVE	DESCRIPTION	KEY POINTS
Malaysia Digital Economy Blueprint (MyDigital)	A strategy for driving Malaysia's digital transformation with six strategic thrusts.	• Target: 70% of companies to adopt cybersecurity by 2025. • Focus on digitalization, data sharing, and skills development. • Promotes innovation and trust.
National Fiberisation and Connectivity Plan (NFCP)	Now known as Jalinan Digital Negara (JENDELA), aims for robust digital infrastructure by 2025.	• 100% digital literacy for civil servants. • Transition 80% of government services online. • Enhances accessibility and efficiency in services.
Digital Trust Model for Digital Prosperity	Introduced by PIKOM, it provides a framework for stakeholders to enhance digital prosperity by 2030.	• Emphasizes technology, talent, collaboration, standardization, and fair trade. • Promotes secure and equitable digital innovations.
Malaysia Cyber Security Strategy (MCSS)	Developed by NACSA to protect against cyberattacks with a medium-term action plan based on five pillars.	• Includes 12 strategies, 35 action plans, and 113 programs. • Focus on improving ICT infrastructure and governance in cybersecurity.
Digital Education Learning in Malaysia (DELIMa)	A Ministry of Education initiative to integrate digital tools into education, enhancing student skills for the digital landscape.	• Utilizes platforms like Google Classroom. • Encourages interactive learning and responsibility in digital interactions. • Prepares students for future challenges.
Building Awareness and Education	Initiatives like the CyberDSA 2024 Forum focus on ethical conduct and transparency in the digital ecosystem.	• Recognizes cybersecurity professionals through awards. • Encourages user experience alongside compliance with regulations. • Implements robust security measures.
Collaborations with International Bodies	Partnerships with Russia and major tech firms like Google to enhance education and boost digital competitiveness.	• Focus on scholarships, research partnerships, and student exchanges. • Google collaboration includes skilling programs and infrastructure investments.

REGULATORY FRAMEWORKS AND LEGISLATION IN ENHANCING DIGITAL TRUST

REGULATORY FRAMEWORK	DESCRIPTION	KEY POINTS
Personal Data Protection Act (PDPA)	Enacted in 2010 and amended in 2024, the PDPA provides guidelines for the collection, use, and storage of personal data to promote accountability and transparency.	Enhances public confidence in digital services. Ensures responsible handling of personal data.
Cyber Security Act 2024	Newly introduced legislation that mandates organizations to follow strict cybersecurity protocols and report incidents to NACSA.	Protects critical information infrastructure. Aims to mitigate cyber threats through a comprehensive legal framework.
Communications and Multimedia Act 1998 (CMA)	Establishes a regulatory framework for communication and multimedia services, promoting a competitive marketplace while ensuring consumer protection.	Regulates online content to enhance digital trust. Supports freedom of expression while holding content creators accountable.
National Digital ID Framework (NDID)	Aims to create a reliable digital identity platform for individuals, organizations, and the government to engage securely in the digital economy.	Enables secure online identity verification. Supports both public and private organizations in authenticating identities for electronic services.
National Cyber Security Policy (NCSP)	A comprehensive framework designed to protect Malaysia's cyber infrastructure and enhance resilience against cyber threats through collaboration among stakeholders.	Promotes a robust cybersecurity culture. Aims to protect critical national information infrastructure (CNII) and enhance public confidence online.
Industry Standards and Certification (ISO/IEC 27001)	Provides a systematic approach to managing sensitive information, ensuring its confidentiality, integrity, and availability through rigorous assessments and audits.	Enhances trust among stakeholders by demonstrating commitment to information security. Supports legal compliance and best practices in data management.

PREDICITVE FACTORS FOR DIGITAL TRUST

In the digital age, trust is paramount for fostering user engagement and ensuring the security of personal information. The concept of digital trust encompasses various factors, including confidence in security measures, satisfaction with cybersecurity protocols, the effectiveness of laws and regulations, understanding responsible online behaviour, ease of information exchange, and confidence in data protection with emerging technologies. Each of these elements plays a crucial role in shaping users' perceptions and experiences in the digital landscape. However, challenges such as low confidence levels, disparities in digital literacy, and the rapid evolution of technology pose significant threats to building a robust framework of digital trust. Addressing these issues through targeted educational initiatives and improved infrastructure is essential for bridging the digital divide and enhancing overall user confidence.

	STRENGTH	WEAKNESS	OPPORTUNITIES	THREATS
CONFIDENCE IN DIGITAL SECURITY MEASURES	Users' belief in data protection systems affects their digital engagement.	Low confidence in security measures persists despite their recognized importance.	Targeted educational initiatives can boost digital literacy, especially in low-confidence areas; higher education correlates with increased trust.	Marginalized communities may lack access to digital education, exacerbating the digital divide; inconsistent internet in rural areas limits educational outreach.
SATISFACTION WITH CYBERSECURITY MEASURES	Higher satisfaction among IT professionals indicates better perceptions of data protection.	Individual experiences shape satisfaction, often influenced by IT backgrounds.	Invest in rural digital infrastructure and awareness programs to enhance overall trust and satisfaction.	Financial limitations may restrict rural infrastructure investments; resistance to new technologies can hinder adoption.
EFFECTIVENESS OF LAWS AND REGULATIONS	Strong regulations promote adherence to data governance, enhancing user confidence.	Under-enforcement and misunderstanding of laws negatively affect trust.	Increase transparency in data practices through clear communication, which can build user confidence.	Scepticism about organizations persists despite transparency efforts, compounded by complex data policies that confuse users.

	STRENGTH	WEAKNESS	OPPORTUNITIES	THREATS
UNDERSTANDING RESPONSIBLE ONLINE BEHAVIOR	Education on online practices boosts user confidence in digital navigation.	Digital literacy disparities limit understanding of responsible behavior, particularly among older demographics.	Public campaigns on responsible online behavior can enhance digital trust and engagement.	Limited engagement from certain demographics may reduce campaign effectiveness and hinder improvements in digital trust.
EASE OF INFORMATION EXCHANGE	Secure information exchange is crucial for user engagement with digital platforms.	Balancing ease of exchange with security is essential; overemphasis on ease can jeopardize data protection.	Implement training programs for non-technical employees to improve organizational digital trust.	Low training participation may occur if relevance is not perceived; budget constraints can limit resource allocation for training.
CONFIDENCE IN DATA PROTECTION WITH EMERGING TECHNOLOGIES	Users generally trust data protection in emerging technologies like AI and cloud computing.	Concerns about data governance in these technologies foster consumer distrust.	Regularly update cybersecurity measures to align with emerging technologies; transparency is key for building user confidence.	Rapid technological changes challenge organizations' ability to maintain current cybersecurity measures, risking public trust.

In conclusion, the path to establishing strong digital trust is fraught with both challenges and opportunities. By prioritizing education on cybersecurity measures and responsible online behaviour, enhancing transparency in data practices, and investing in digital infrastructure–especially in underserved communities–stakeholders can significantly improve users' confidence in digital environments. As technology continues to advance at a rapid pace, it is imperative that organizations remain proactive in updating their cybersecurity measures and regulations to maintain public trust. Ultimately, fostering a culture of awareness and engagement will not only empower individuals to navigate the digital landscape safely but also create a more secure and trustworthy online ecosystem for all.

Challenges and Opportunities

While Malaysia has made progress in building digital trust, challenges such as **low public awareness**, **fragmented implementation**, and **rapid technological change** must be addressed. Opportunities lie in strengthening cybersecurity frameworks, enhancing data protection regulations, and fostering international collaboration.

Core Components Digital Trust for Malaysia

Building a robust digital trust ecosystem in Malaysia requires a multifaceted approach that integrates international best practices with local nuances. The following core components are essential for fostering digital trust, ensuring that the digital landscape is secure, transparent, and user-centric

- **CYBERSECURITY**

  At the heart of digital trust lies cybersecurity, which encompasses robust and proactive measures designed to protect against cyber threats and vulnerabilities. Organizations must implement comprehensive security frameworks that not only defend against attacks but also foster a culture of vigilance among users. This proactive stance is critical in mitigating risks and enhancing user confidence in digital services.

- **DATA PROTECTION**

  Data protection is another fundamental pillar, involving comprehensive laws and practices that ensure the privacy and security of personal and organizational data. Malaysia must prioritize the establishment of strong data protection regulations that align with international standards while addressing local challenges. This includes safeguarding sensitive information, particularly as emerging technologies like AI and blockchain become more prevalent.

- **TRANSPARENCY**

  Transparency is vital for building trust. Clear and open communication regarding data use, security practices, and governance fosters an environment where users feel informed and empowered. Organizations should adopt transparent policies that allow users to understand how their data is handled, thereby reinforcing their confidence in digital systems.

➢ DIGITAL TRUST ACCULTURATION

To cultivate a culture of trust, digital trust acculturation is essential. This involves educating citizens about digital trust matters, including cybersecurity, data privacy, and responsible online behavior. By fostering awareness and understanding, Malaysia can create a populace that values digital trust as a cornerstone of its digital economy.

➢ INTERNATIONAL COLLABORATION:

In an interconnected world, international collaboration is crucial. Participation in global initiatives allows Malaysia to adhere to consistent digital trust and cybersecurity standards. Collaborative efforts can enhance knowledge sharing, improve regulatory practices, and address common challenges faced by nations in the digital arena.

➢ LOCAL CONTEXT

Recognizing the local context is imperative for effective implementation of digital trust strategies. This includes promoting responsible online behavior among Malaysians and ensuring interoperability within the Malaysian digital ecosystem. Tailoring approaches to meet specific cultural and societal needs will enhance the effectiveness of digital trust initiatives.

➢ HUMANIZING DIGITAL TRUST

A transformative aspect of building digital trust is the humanizing element that emphasizes understanding individual experiences and concerns in the digital landscape. This perspective acknowledges that behind every data point is a person with unique vulnerabilities and rights. By prioritizing empathy and user-centric approaches, organizations can foster a culture of responsibility that resonates with users' lived realities. Encouraging open dialogue about data sharing, privacy, and security will lead to compassionate solutions that empower individuals to navigate the digital world confidently.

GLOBAL PERSPECTIVE	MALAYSIAN PERSPECTIVE
• **Cybersecurity:** Robust and proactive measures to protect against cyber threats and vulnerabilities. • **Data Protection:** Comprehensive laws and practices ensure personal and organizational data privacy and security. • **Transparency:** Clear and open communication regarding data use, security practices, and governance. • **Digital Trust Acculturation:** Educating citizens about digital trust matters, fostering a culture of trust and awareness. • **International Collaboration:** Participation in global initiatives to adhere to international digital trust and cybersecurity standards.	• **Security Measures:** Security measures protecting personal data when using digital services in Malaysia. • **Cybersecurity Measures:** Cybersecurity measures implemented by Malaysian organizations to prevent data breaches. • **Data Protection:** Malaysian organizations' ability to protect your data and confidentiality while using emerging technologies like AI and blockchain. • **Laws and Regulation:** Malaysia's current laws and regulations at protecting your digital information and online confidentiality. • **Responsible in Online Data Sharing:** Malaysians understand and adhere to responsible online behavior and data sharing practices. • **Connect Exchange Info:** Seamless connect and exchange information across different Malaysian digital platforms or services.

Mapping on Digital Trust Ecosystem based on International and Malaysian Public Opinion

In summary, the core components of digital trust in Malaysia must integrate technological advancements with a deep understanding of human factors and societal dynamics. By emphasizing user trust through safe technologies, promoting community interaction, and implementing supportive regulations, Malaysia can cultivate an ecosystem that enhances digital trust. This holistic approach not only improves user acceptance but also contributes to the overall success and sustainability of digital initiatives. Ultimately, aligning foundational elements such as cybersecurity, data protection, transparency, and international collaboration with local nuances will create a more secure digital ecosystem that protects data while fostering trust among users.

Challenges to Digital Trust in Malaysia

As Malaysia navigates a rapidly evolving digital landscape, it faces a dual-edged sword of opportunities and challenges in cultivating digital trust. While global frameworks identify critical issues, the Malaysian context demands a more nuanced approach that goes beyond cybersecurity to encompass socio-political, cultural, and regulatory dimensions. Below are the pressing challenges to digital trust based on the analysis of global frameworks and which are very relevant for Digital Trust in Malaysia moving forward.

○ Insufficient Integration of Socio-Political and Human Factors

Current digital trust frameworks often overlook the intricate socio-political landscape and the human elements that shape user behavior. This disconnect can severely impede the effective implementation and acceptance of digital systems among users.

○ Erosion of Institutional Trust

The waning trust in public Institutions—aggravated by political instability and corruption—poses a formidable barrier to fostering confidence in digital systems. This erosion breeds scepticism about the security and reliability of digital platforms, undermining their potential benefits.

○ Complexity of Digital Interactions

As digital transactions grow increasingly intricate, users may struggle to navigate these systems effectively. This complexity can lead to frustration and disengagement, ultimately eroding trust in the very platforms designed to enhance convenience.

○ Rapid Technological Change

The relentless pace of technological Innovation presents significant challenges for regulatory bodies striving to keep laws relevant. This gap can result in outdated protections that fail to safeguard against emerging threats, leaving users vulnerable.

- **Vulnerability to Cyber Threats**

While cybersecurity remains a critical concern, an exclusive focus on this area may obscure broader issues that impact digital trust. Persistent cyberattacks not only expose vulnerabilities but also highlight the need for a more holistic understanding of trust that encompasses ethical practices and user empowerment.

- **Fragmented Implementation Across Sectors**

The inconsistent application of digital trust measures across various sectors leads to disparate levels of security and reliability. This fragmentation creates confusion for users who interact with multiple platforms, diminishing their overall confidence in digital services.

- **Challenges in Measuring Trust**

Quantifying digital trust is an inherently complex endeavor, complicating policy assessments and obscuring areas in need of improvement. Without clear metrics, it becomes challenging to track progress or identify successful strategies.

- **Cultural Differences in Trust Perception**

Trust perceptions differ markedly across Malaysia's diverse cultural contexts. A one-size-fits-all approach is inadequate; tailored strategies are essential to address the unique needs and concerns of various communities effectively.

To overcome these challenges, Malaysia must adopt a comprehensive and inclusive strategy that enhances cybersecurity, cultivates transparency, and empowers users. Collaboration between government, businesses, and civil society is essential for building a resilient digital trust framework.

As the nation embraces digital transformation, fostering trust will be essential in unlocking the full potential of technology, driving innovation, and ensuring that all citizens feel secure and confident in engaging with digital platforms. In doing so, Malaysia can position itself as a leader in the global digital economy, where trust serves as the foundation for sustainable growth and societal progress.

Opportunities for Strengthening Digital Trust in Malaysia

The evolving landscape of digital trust in Malaysia presents numerous opportunities for enhancing cybersecurity and data protection, driven by key initiatives such as the Malaysia Cyber Security Strategy (MCSS) and the amended Personal Data Protection Act (PDPA). With increased investment in cybersecurity infrastructure, organizations can bolster their defences against sophisticated cyber threats, fostering a more resilient digital environment.

The MCSS outlines strategic pillars aimed at improving national governance and management of cybersecurity risks, which not only enhances the security posture of critical national information infrastructure but also encourages public-private partnerships to share resources and expertise in combating cyber threats. This collaborative approach is essential for building a robust cybersecurity culture that can adapt to emerging challenges.

Apart from that, the introduction of stricter regulations under the amended PDPA, including mandatory data breach notifications and penalties for non-compliance, offers a significant opportunity to improve public trust in digital services. By establishing clear accountability and governance frameworks, organizations can enhance their compliance mechanisms, thereby fostering a culture of transparency and responsibility in handling personal data. The potential for data protection certifications also emerges as a means to instil confidence among consumers, encouraging them to engage more actively with digital platforms. This regulatory environment not only protects individuals but also creates a competitive advantage for businesses that prioritize data security and privacy.

Lastly, international collaborations and regional initiatives, such as partnerships with tech companies and ASEAN cybersecurity cooperation strategies, present avenues for knowledge exchange and innovation in digital technologies. The establishment of the National AI Office and the promotion of ethical AI practices signal Malaysia's commitment to integrating advanced technologies responsibly while ensuring that they align with public trust principles. By leveraging these opportunities, Malaysia can position itself as a leader in digital trust within the ASEAN region, contributing to a secure and prosperous digital economy that benefits all stakeholders involved.

In conclusion, while Malaysia stands at a pivotal juncture in its pursuit of enhancing digital trust through strategic initiatives and regulatory frameworks, the journey is fraught with challenges that must be addressed to fully realize these opportunities. Budgeting constraints, a lack of awareness and compliance among organizations, and a significant skills gap in the cybersecurity workforce pose substantial hurdles that can undermine the effectiveness of newly implemented measures. To build a secure and trusted digital environment, it is imperative for stakeholders including government bodies, businesses, and educational institutions to collaborate effectively, invest in cybersecurity infrastructure, and prioritize the development of a knowledgeable workforce. By overcoming these challenges, Malaysia can not only strengthen its digital trust framework but also position itself as a leader in the ASEAN region's digital economy, fostering innovation and consumer confidence in an increasingly interconnected world.

KEY OPPORTUNITIES

Enhancing Data Protection Regulation

Update existing laws to reflect current technological realities and ensure compliance with global standards

Promoting Transparency and Accountability

Mandate organizations to disclose their data handling practices clearly

Cultivating Digital Literacy

Launch nationwide initiatives to enhance digital literacy across all demographics

Strengthening Cybersecurity Frameworks

Develop comprehensive cybersecurity policies that align with international standards

Encouraging Public-Private Partnerships

Collaborate with private sector stakeholders to develop innovative solutions

Establishing a National Digital Trust Centre

Create a dedicated entity responsible for overseeing digital trust initiatives

International Collaboration

Engage in global partnerships to share best practices and address cross-border cyber threats

Case Study and Global Benchmark

Building Malaysia's National Digital Trust Framework: Insights from Global Models

In an era of rapid digital transformation, trust is the foundation of a thriving digital economy. Global frameworks provide valuable insights into establishing a robust National Digital Trust Framework for Malaysia. The following key models highlight critical components of digital trust and what Malaysia can adopt to strengthen its digital ecosystem

Key Components of Leading Digital Trust Frameworks

1. **PwC's Global Digital Trust Insights, 2024 –** Emphasizes the need for effective cybersecurity investments and the challenge of measuring their success. Trust is built not just through spending but by ensuring cybersecurity measures are impactful.
2. **ISACA's The State of Digital Trust 2024 –** Highlights the gap between recognizing digital trust as crucial and actual investment in trust-building initiatives. Organizations must integrate trust into their core digital strategies.
3. **Thales 2024 Trust Index Ranking** – Reveals that banks, healthcare, and governments rank highest in trust, while media lags behind. A strong governance structure is key to ensuring trust across industries.
4. **McKinsey's Why Digital Trust Truly Matters 2022** – Demonstrates that strong digital trust enhances business growth and consumer confidence. Businesses that prioritize trust experience higher customer retention and market success.
5. **Digital Intelligence Index, Tufts University, 2020** – Ranks economies based on digital readiness and trustworthiness, emphasizing that a nation's economic resilience is linked to digital trust levels.
6. **World Economic Forum Digital Trust Framework** – Defines core trust principles to assess digital technology integrity, advocating for transparency, security, and accountability as key trust pillars.
7. **PIKOM Digital Trust Model for Digital Prosperity** – Focuses on innovation, governance, and collaboration as critical elements for fostering digital trust in a technology-driven economy.

What Malaysia Can Replicate and Adopt

To establish a world-class **National Digital Trust Framework**, Malaysia can integrate the following key principles:

a) Security & Cyber Resilience – Prioritize impactful cybersecurity investments and ensure their effectiveness, as highlighted by PwC and ISACA.
b) Governance & Regulation – Build trust through strong regulatory frameworks that support financial, healthcare, and government sectors, aligning with Thales' trust rankings.
c) Economic Growth through Trust – Recognize digital trust as an economic enabler, fostering business confidence and international competitiveness, as emphasized by McKinsey and Tufts University.
d) Transparency & Ethical Standards – Align with global trust principles from the **World Economic Forum** to enhance trust in digital services.
e) Innovation & Collaboration – Foster digital trust through **public-private partnerships and cross-industry collaboration**, as advocated in the PIKOM model.

By integrating these elements, Malaysia can develop a **future-ready, inclusive, and globally recognized Digital Trust Framework** that strengthens its digital economy and national resilience

GLOBAL BEST PRACTICES IN DIGITAL TRUST: KEY SUCCESS FACTORS FOR MALAYSIA

As Malaysia develops its **National Digital Trust Framework**, learning from global leaders in digital trust is essential. Countries & Regions such as The **European Union, Estonia, Germany, South Korea, Canada, Finland, and Singapore** have successfully built robust digital ecosystems. Their success is driven by a combination of **strong governance, cybersecurity frameworks, data protection policies, and digital innovation**.

BUILDING A TRUSTED DIGITAL NATION: KEY LESSONS FROM DIGITAL TRUST LEADERS

1. Seamless & Secure Digital Identity

Estonia's **e-Estonia and X-Road** have set the gold standard for **secure, seamless digital identity and interoperability**. Malaysia should implement a **national digital identity system** to enhance trust in e-government and digital transactions.

2. Comprehensive Data Protection & Cybersecurity

Strong data protection policies like **EU's GDPR, South Korea's Personal Information Protection Commission, and Canada's PIPEDA** ensure digital trust. Malaysia must adopt **stringent data privacy laws** and strengthen enforcement through a centralized **cybersecurity agency** like Finland's **NCSC-FI**.

3. National Cybersecurity Strategy & Governance

Leading countries have **dedicated cybersecurity agencies** such as **Canada's CCCS and Finland's NCSC-FI** that provide national oversight. Malaysia should establish a **centralized cybersecurity authority** to enforce regulations, combat cyber threats, and protect national digital infrastructure.

4. Digital Economy & Smart Nation Vision

Singapore's **Smart Nation Initiative** and Germany's **Digital Strategy 2025** emphasize **innovation, digital infrastructure, and regulatory frameworks** to drive economic growth. Malaysia must **align digital trust with its national digital economy strategy** to attract investments and enhance global competitiveness.

5. Resilient & Decentralized Data Infrastructure

Estonia's **Data Embassy** and Singapore's **Digital Trust Centre** enhance **data sovereignty and security**. Malaysia should develop **secure cross-border data storage and trusted digital infrastructure** to build resilience against cyber threats.

6. Comprehensive legal Framework (European Union)

The European Union (EU) Digital Decade Strategy, set to guide Europe through the digital transformation by 2030, outlines ambitious goals to ensure the region leads in digital technology while safeguarding fundamental values. The strategy focuses on four key areas: empowering citizens with digital skills, expanding digital infrastructure, ensuring digital sovereignty, and enhancing the digital economy. The goal is to achieve a green, digital, and resilient Europe, with specific targets, such as widespread access to fast internet, enhancing cybersecurity, and fostering the development of artificial intelligence (AI). The strategy emphasizes inclusivity, ensuring that digital advancements benefit everyone while minimizing inequalities across regions and social groups. To support these objectives, several EU laws have been introduced to build and sustain Digital Trust across Europe including, Cyber Resilience Act, AI Act, Data Governance Act, GDPR (General Data Protection Regulation), Digital Services Act (DSA) and Digital Markets Act (DMA). Together, these EU regulations provide a comprehensive legal framework that enhances digital trust by ensuring security, privacy, fairness, and transparency across digital systems. By addressing various aspects of digital technology, from cybersecurity and data privacy to AI ethics and platform fairness, they collectively contribute to a safer, more transparent, and accountable digital environment for European citizens and businesses. This legal framework plays a critical role in fostering trust, which is essential for the widespread adoption of digital technologies and innovations.

MALAYSIA'S PATH FORWARD: BUILDING A SUSTAINABLE DIGITAL TRUST ECOSYSTEM

As Malaysia advances towards becoming a leading digital economy, building a sustainable digital trust ecosystem is paramount. Trust is the foundation of a thriving digital landscape, ensuring security, inclusivity, and innovation. To achieve this, Malaysia must integrate a three-pronged approach that balances technology, governance, and user experience.

a) **TECHNOLOGY-CENTRIC APPROACH –** Malaysia must enhance security, privacy, and the reliability of digital technologies by adopting cutting-edge cybersecurity frameworks, AI-driven threat detection, and trusted digital infrastructure. Strengthening national cybersecurity policies and developing secure digital identity systems will be critical to fostering confidence in digital transactions and services.

b) **SOCIO-POLITICAL APPROACH –** A strong digital trust framework must align with regulatory frameworks, societal norms, and cultural expectations. By establishing clear data protection laws, ethical AI governance, and transparent regulatory oversight, Malaysia can enhance public confidence and international credibility. Partnerships between the public and private sectors will be vital to fostering a resilient digital trust ecosystem.

c) **USER-CENTRIC APPROACH** – Digital trust must ultimately serve the people. Prioritizing user experience, accessibility, and digital literacy will ensure that all Malaysians, regardless of background, can safely and confidently participate in the digital economy. This includes nationwide digital literacy programs, user-friendly digital services, and greater inclusivity for underserved communities.

A FUTURE BUILT ON TRUST

By integrating these three approaches, Malaysia can create a secure, inclusive, and innovation-driven digital ecosystem. A robust digital trust framework will attract investment, strengthen economic resilience, and position Malaysia as a global leader in digital trust. As the nation moves forward, fostering trust in technology, governance, and user experience will be the key to unlocking Malaysia's digital potential.

The Future of Digital Trust Malaysia

As Malaysia accelerates its digital transformation, the foundation of its success lies in fostering **Digital Trust**—a secure, inclusive, and innovative ecosystem that empowers all Malaysians. Digital Trust is more than just a technological requirement; it is a national imperative that strengthens **cybersecurity resilience, economic growth, and public confidence in digital services**.

To achieve this, Malaysia must prioritize **strong cybersecurity measures, ethical governance of emerging technologies, and robust data protection frameworks**. These elements will ensure that individuals, businesses, and government institutions can operate in a digital environment that is both secure and transparent. By enforcing **clear laws and regulations**, encouraging **responsible online data sharing**, and promoting **standards and interoperability**, Malaysia can establish a digital ecosystem that fosters **trust, innovation, and competitiveness** on the global stage.

Digital Trust is a shared responsibility that requires active participation from all sectors. The **government** plays a key role in enhancing digital infrastructure, strengthening security, and ensuring regulatory compliance. **Businesses** must embrace cybersecurity best practices to protect consumers and enhance customer trust, while continuously innovating to remain competitive. The **rakyat (citizens)**, as the backbone of this digital society, must be equipped with the knowledge and tools to navigate the digital landscape safely, fostering a culture of digital inclusion and empowerment.

By **enhancing infrastructure, building cyber resilience, and developing future digital talent**, Malaysia can position itself as a leader in the digital economy. A future driven by Digital Trust will not only **safeguard national security and data sovereignty** but will also unlock new economic opportunities, drive innovation, and create a society where every Malaysian can thrive in the digital era.

With a collective commitment to strengthening Digital Trust, Malaysia is poised to **build a resilient, secure, and thriving digital nation**, shaping a future where technology serves as a catalyst for progress, prosperity, and inclusivity.

EMERGING TRENDS SHAPING DIGITAL TRUST

1. Cybersecurity Threats and Resilience

- **Trend**: Increasingly sophisticated cyberattacks, including ransomware, phishing, and state-sponsored threats.
- **Impact on Digital Trust**: Heightens the need for robust cybersecurity measures, public awareness, and trust in digital systems.
- **Malaysia's Context**: The Malaysia Cyber Security Strategy and organisations like CyberSecurity Malaysia are critical to building resilience and public confidence.

2. Data Privacy and Protection

- **Trend**: Growing concerns over data breaches, misuse of personal data, and compliance with regulations like GDPR and Malaysia's **Personal Data Protection Act (PDPA)**.
- **Impact on Digital Trust**: Strengthening data protection frameworks and ensuring transparency in data handling are essential for trust.
- **Malaysia's Context**: Updates to the PDPA and alignment with international standards are key to fostering trust in digital services.

3. Artificial Intelligence (AI) and Ethical AI Deployment

- **Trend**: Rapid adoption of AI in industries, coupled with concerns over bias, accountability, and ethical use.
- **Impact on Digital Trust**: Ethical AI frameworks and transparency in AI decision-making are crucial for public acceptance.
- **Malaysia's Context**: The **National AI Framework** and ethical guidelines for AI use are shaping trust in AI-driven solutions.

4. Digital Identity and Authentication

- **Trend**: Adoption of secure digital identity systems, including biometrics and blockchain-based solutions.
- **Impact on Digital Trust**: Reliable and secure digital identity systems enhance trust in online transactions and government services.
- **Malaysia's Context**: Initiatives like **MyDigital ID** and the **National Digital Identity Framework** are pivotal for secure digital interactions.

5. Internet of Things (IoT) and Connected Devices

- **Trend**: Proliferation of IoT devices in homes, industries, and cities.
- **Impact on Digital Trust**: Ensuring the security and privacy of connected devices is critical to prevent vulnerabilities.

- **Malaysia's Context**: Smart city projects and IoT adoption in industries require robust security standards to build trust.

6. Blockchain and Decentralized Technologies

- **Trend**: Growing use of blockchain for transparency, security, and trust in transactions.
- **Impact on Digital Trust**: Blockchain's immutability and transparency can enhance trust in financial, supply chain, and government systems.
- **Malaysia's Context**: Blockchain adoption in sectors like finance (e.g., Bank Negara's Project Dunbar) and supply chains is fostering trust in digital transactions.

7. 5G and Next-Gen Connectivity

- **Trend**: Rollout of 5G networks enabling faster, more reliable connectivity.
- **Impact on Digital Trust**: Enhanced connectivity must be paired with strong security measures to prevent new vulnerabilities.
- **Malaysia's Context**: The **National 5G Task Force** and Digital Nasional Berhad (DNB) are driving 5G adoption, requiring trust-building measures.

8. Digital Inclusion and Accessibility

- **Trend**: Efforts to bridge the digital divide and ensure equitable access to digital services.
- **Impact on Digital Trust**: Inclusive digital transformation fosters trust among all demographics, including rural and underserved communities.
- **Malaysia's Context**: Initiatives like **JENDELA** and the **Malaysia Digital Economy Blueprint** aim to ensure no one is left behind.

9. Regulatory Evolution and Harmonization

- **Trend**: Updating and harmonizing regulations to keep pace with technological advancements.
- **Impact on Digital Trust**: Clear, consistent, and enforceable regulations build confidence in digital systems.
- **Malaysia's Context**: Updates to the **Communications and Multimedia Act 1998** and alignment with international frameworks are key.

10. Public Awareness and Digital Literacy

- **Trend**: Increasing emphasis on educating the public about cybersecurity, data privacy, and responsible digital behavior.
- **Impact on Digital Trust**: An informed public is better equipped to engage safely and confidently in the digital ecosystem.

- **Malaysia's Context**: Programs like **CyberSAFE** and digital literacy campaigns are essential for building trust.

11. Sustainability and Green Digital Technologies

- **Trend**: Growing focus on sustainable and energy-efficient digital technologies.
- **Impact on Digital Trust**: Trust in digital systems is enhanced when they align with environmental and social values.
- **Malaysia's Context**: Green tech initiatives and sustainable digital transformation efforts are gaining traction.

12. Cross-Border Data Flows and Sovereignty

- **Trend**: Increasing importance of managing cross-border data flows while ensuring data sovereignty.
- **Impact on Digital Trust**: Balancing global connectivity with national security and privacy concerns is critical for trust.
- **Malaysia's Context**: Policies on data localization and international data-sharing agreements are shaping trust in global digital interactions.

13. Rise of Deepfakes and Misinformation

- **Trend**: Proliferation of deepfakes, fake news, and misinformation campaigns.
- **Impact on Digital Trust**: Combating misinformation is essential to maintain trust in digital content and platforms.
- **Malaysia's Context**: Efforts like the **Sebenarnya.my** and media literacy programs are addressing this challenge.

14. Cloud Computing and Edge Computing

- **Trend**: Adoption of cloud and edge computing for scalable, efficient digital services.
- **Impact on Digital Trust**: Ensuring the security and reliability of cloud-based systems is vital for trust.
- **Malaysia's Context**: Cloud adoption in government (e.g., **MyGovCloud**) and industries requires robust trust-building measures.

15. Digital Payments and Fintech Innovation

- **Trend**: Growth of digital payments, e-wallets, and fintech solutions.
- **Impact on Digital Trust**: Secure and seamless digital payment systems enhance trust in financial transactions.
- **Malaysia's Context**: Initiatives like **DuitNow** and the rise of e-wallets (e.g., GrabPay, Touch 'n Go eWallet) are transforming the financial landscape.

These trends highlight the multifaceted nature of Digital Trust and its importance in shaping Malaysia's digital future. Addressing these trends through policy, innovation, and collaboration will be key to building a trusted and resilient digital ecosystem.

LONG-TERM VISION FOR MALAYSIA'S DIGITAL ECOSYSTEM

The long-term vision for Malaysia's digital ecosystem is to create an environment where all stakeholders—government entities, businesses, and citizens—can engage confidently in digital interactions. This ecosystem will prioritize:

USER-CENTRIC DESIGN

- Digital services must be designed with user needs at the forefront. By prioritizing usability and accessibility, Malaysia can enhance user experiences and build trust in digital platforms.

RESILIENCE AGAINST CYBER THREAT

- A proactive approach to cybersecurity will be essential. Building resilient infrastructures capable of withstanding cyberattacks will reinforce public confidence in digital services.

ETHICAL GOVERNANCE

- Establishing ethical guidelines for technology use will ensure that innovations are developed responsibly. This governance framework will address issues such as data privacy, consent management, and algorithmic accountability.

INCLUSIVE PARTICIPATION

- Ensuring that all segments of society can participate in the digital economy is vital for building trust. Initiatives aimed at increasing digital literacy among marginalized communities will empower citizens to navigate online spaces safely.

STRATEGIC GOALS FOR ENHANCING DIGITAL TRUST (2025-2035)

To realize this vision, Malaysia must set clear strategic goals over the next decade:

STRENGTHENING CYBERSECURITY FRAMEWORKS

Develop comprehensive cybersecurity policies that align with international standards while focusing on local contexts. This includes implementing a zero-trust security model that continuously verifies user identities and access rights.

ENHANCING DATA PROTECTION REGULATIONS

Update existing data protection laws to reflect current technological realities while ensuring compliance with global standards such as the General Data Protection Regulation (GDPR). This will involve creating clear guidelines on data collection, usage, and user rights.

PROMOTING TRANSPARENCY AND ACCOUNTABILITY

Foster an environment of transparency by mandating organizations to disclose their data handling practices clearly. Public awareness campaigns should educate citizens about their rights regarding data privacy and security.

CULTIVATING DIGITAL LITERACY

Launch nationwide initiatives to enhance digital literacy across all demographics. By equipping citizens with the skills needed to navigate online environments safely, Malaysia can empower individuals to engage confidently in the digital economy.

ENCOURAGING PUBLIC-PRIVATE PARTNERSHIPS

Collaborate with private sector stakeholders to develop innovative solutions that enhance digital trust. These partnerships can facilitate knowledge sharing and resource allocation necessary for implementing effective cybersecurity measures.

ESTABLISHING A NATIONAL DIGITAL TRUST CENTRE

Create a dedicated entity responsible for overseeing digital trust initiatives across sectors. This center would serve as a hub for research, policy development, and public engagement efforts aimed at strengthening digital trust nationwide.

INTERNATIONAL COLLABORATION

Engage in global partnerships to share best practices related to cybersecurity and data protection. By participating in international forums focused on digital trust, Malaysia can align its strategies with global trends while addressing cross-border cyber threats effectively.

The future of digital trust in Malaysia hinges on the nation's ability to adapt to emerging technologies while addressing the challenges they present. By embracing AI, blockchain, and 5G within a framework of robust cybersecurity measures and ethical governance, Malaysia can cultivate an environment where all stakeholders feel secure engaging in digital interactions.

As the nation sets its sights on enhancing digital trust over the next 5-10 years through strategic goals focused on cybersecurity resilience, data protection regulations, transparency initiatives, public education programs, public-private partnerships, and international collaboration, it will lay the foundation for a thriving digital ecosystem that empowers government entities, businesses, and citizens alike.

In doing so, Malaysia not only positions itself as a leader in the regional digital economy but also ensures that its citizens can confidently navigate an increasingly complex digital landscape—ultimately fostering innovation while safeguarding privacy and security for all stakeholders involved.

Conclusion

STRENGTHENING DIGITAL TRUST: A HOLISTIC APPROACH FOR MALAYSIA

The interplay between **Digital Trust** and a comprehensive societal approach is defined by the **collaborative development of trust-building mechanisms** across various levels. This dynamic encompasses **technological, socio-political, and human aspects** of digital transformation. Fostering a culture of trust is vital to ensuring that digital technologies serve as catalysts for **social cohesion and economic growth**, rather than sources of division and mistrust.

A **strong regulatory foundation** is crucial for digital trust to thrive. **Reviewing existing Digital Trust-related Acts and Laws, updating key regulations such as the DSA 1997, and harmonizing national policies with international frameworks** will create a robust legal environment that protects users and businesses alike. These regulatory measures will enhance **data protection, privacy, and accountability**, ensuring that digital interactions remain **secure, ethical, and transparent**.

Beyond regulations, establishing **standards and certification** is critical to fostering trust. The **adoption of minimum security and compliance standards, the implementation of a voluntary industry Code of Conduct, and the introduction of the Malaysia Digital Trust Maturity Metrics** will provide organizations with clear guidelines to uphold best practices. These initiatives will help strengthen **consumer confidence, encourage ethical technology deployment, and support industry-wide efforts toward cybersecurity resilience**.

To measure and improve trust, Malaysia must **establish a National Digital Trust Index**, serving as a benchmark to assess the nation's progress in building a secure digital environment. This index will **set a national baseline on digital trust and provide regular updates**, offering the public and businesses clear insights into Malaysia's cybersecurity posture and regulatory advancements. By maintaining **transparency and accountability**, the index will enhance public confidence in digital services and foster greater adoption of digital solutions.

However, **building digital trust goes beyond policies and frameworks—it requires a cultural shift**. The **development and employment of a Certified Digital Trust Workforce** will equip professionals with the expertise to safeguard digital ecosystems.

Furthermore, **public awareness campaigns and stakeholder engagement initiatives** will play a crucial role in educating individuals and organizations on responsible digital behavior, cybersecurity best practices, and data protection measures.

In Malaysia, the success of **Digital Trust** depends on **collaboration** between **government agencies, industry players, and the public**. A secure digital ecosystem must **harmonize technological advancements with human-centric policies**, ensuring that digital transformation **empowers citizens, strengthens businesses, and enhances trust in government services**.

To ensure the successful implementation of Malaysia's digital trust agenda, the establishment of a **dedicated central authority**, such as the **Malaysian Digital Trust Centre (MDTC)**, is essential. The MDTC would oversee regulatory harmonization, enforce compliance with digital trust standards, and drive public-private collaboration. It would address challenges like cybersecurity threats, data privacy, and ethical technology deployment while aligning with international best practices. The MDTC would also coordinate the National Digital Trust Index, certify the Digital Trust Workforce, and lead nationwide awareness campaigns. By fostering transparency, accountability, and innovation, the MDTC would build a resilient digital ecosystem, inspiring confidence among citizens, businesses, and global partners, and positioning Malaysia as a regional leader in digital trust.

By **integrating regulatory frameworks, enforcing standards, measuring trust through national indices, and fostering digital awareness**, Malaysia can **pave the way for a resilient, inclusive, and globally competitive digital economy**. This comprehensive approach will not only safeguard national security and data sovereignty but also inspire confidence in digital services, drive innovation, and unlock new economic opportunities. With a steadfast commitment to Digital Trust, Malaysia is well-positioned to lead in the digital era, ensuring a safer and more prosperous future for all.

Annex

Legislation and Policies

Malaysia	
Legislation	Cyber Security Act 2024 (Act 854)
	Personal Data Protection Act 2010 (2024) (Act 709)
	Electronic Commerce Act 2006 (Act 658)
	Communications and Multimedia Act 1998 (Act 588)
	Digital Signature Act 1997 (Act 562)
	Computer Crimes Act 1997 (Act 563)
	Official Secrets Act 1972 (Act 88)
	Consumer Protection Act 1999 (CPA)
	Consumer Protection (Electronic Trade Transactions) Regulations 2012
	Online Safety Act (In Progress)
	Data Sharing Act (In Progress)
	Act 680 Electronic Government Activities Act 2007 (JDN)
National policies	Malaysia Digital Economy Blueprint
	National Fourth Industrial Revolution (4IR) Policy
	National Fiberisation and Connectivity Plan (NFCP)
	Malaysia Cyber Security Strategy (MCSS)
	National Cryptography Policy (NCP)
	National CyberSecurity Awareness Masterplan
	National Digital ID Framework (NDID)
	National Cyber Security Policy (NCSP)
International	
Legislation	Digital Services Act (DSA) – 2022 [EU]
	Digital Markets Act (DMA) – 2022 [EU]
	Online Safety Act 2023 [UK]
	Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) 2022 [USA]
	Digital Personal Data Protection Act, 2023 [India]
	Protection from Online Falsehoods and Manipulation Act (POFMA) – 2019 [Singapore]
	Digital Identity Services Trust Framework Act 2023 [New Zealand]
	Artificial Intelligence Act - 2024 [EU]
	Digital Operational Resilience Act (DORA) 2025 [EU]
	Markets in Crypto-Assets Regulation (MiCA) - 2023 [EU]

	Cyber Resilience Act – 2024 [EU]
	Data Act – 2024 [EU]
	Data Governance Act - 2022 [EU]
Regulations & policies	General Data Protection Regulation (GDPR) – 2018 [EU]
	eIDAS Regulation (Electronic Identification, Authentication and Trust Services) – 2023 [EU]
	European Digital Identity (EUDI) Regulation (Regulation (EU) 2024/1183
	Generative AI Measures (2023) [China]
	Regulation on Cross-Border Transfer of Personal Data 2024 [Turkey]
	NIS2 Directive (Network and Information Security Directive 2022) [EU]
	EU-US Data Privacy Framework - 2023

Digital Trust Legislation & Policies – Brief Comparison

	Singapore	**Japan**	**United Kingdom**
Legislation /Policies/ Strategies	Cybersecurity (Amendment) Act 2024	Basic Act on Cybersecurity	UK General Data Protection Regulation (UK GDPR)
	National AI Strategy 2.0	Telecommunication Business Act	Data Protection Act 2018
	Personal Data Protection Act 2012	Act on the Protection of Personal Information	Networks and Information Systems (NIS) Directive
	Computer Misuse Act 1993	Cybersecurity Strategy 2021	Government Cyber Security Strategy 2022–2030
	Upcoming Digital Infrastructure Act (DIA)		
Agencies	Cyber Security Agency of Singapore (CSA)	National Center of Incident Readiness and Strategy for Cybersecurity (NISC)	National Cyber Security Center
	Digital Trust Center	Digital Agency	

Overview of Malaysia's Digital Trust Legislation and Relevant International Innovations

Area	Malaysia's Current Laws	International Innovations to Consider
Digital Identity	MyDigital ID, ECA 2006	EU's eIDAS 2.0, Singapore's Singpass
Cybersecurity	Cyber Security Act 2024	EU's NIS2, US CIRCIA
Data Privacy	PDPA 2010 (Limited Enforcement)	GDPR, Singapore's PDPA 2020
Blockchain/Crypto	SC & BNM Guidelines (Fragmented)	EU MiCA, UAE Virtual Assets Law
AI Governance	No Specific Law	EU AI Act, China Generative AI Rules

Standard and Certification

Information Security Standards	ISO/IEC 27001 – Information Security Management System (ISMS)
	ISO/IEC 27002 – Code of Practice for Information Security Controls
	ISO/IEC 27005 – Information Security Risk Management
	ISO/IEC 15408 Common Criteria
	NIST Cybersecurity Framework (CSF)
	COBIT 2019 – Governance and Management of Enterprise IT
	CSA STAR Certification – Cloud Security Alliance Security Trust Assurance & Risk
	TISAX – Trusted Information Security Assessment Exchange (automotive industry)
Privacy and Data Protection	ISO/IEC 27701 – Privacy Information Management System (extension of ISO 27001)
	ISO/IEC 29100 – Privacy Framework
	ISO/IEC 29134 – Privacy Impact Assessment
	EU GDPR Compliance Certifications (e.g., EuroPriSe, BS 10012)
	APEC Cross Border Privacy Rules (CBPR)
	NIST Privacy Framework
	Malaysia PDPA Compliance Framework (Act 709)

Digital Identity And Authentication	ISO/IEC 24760 – Framework for Identity Management
	ISO/IEC 29115 – Entity Authentication Assurance
	NIST SP 800-63 – Digital Identity Guidelines
	eIDAS Regulation (EU) – Electronic Identification and Trust Services
	FIDO2/WebAuthn – Strong Authentication Standards
	MyDigital ID (Malaysia) – National Identity Initiative
Trust Services And Digital Signatures	eIDAS (EU) – Legal framework for trust services
	IETSI EN 319 401-421 – Electronic Signatures and Trust Services Standards
	WebTrust for Certification Authorities – Assurance for Cas
	CA/Browser Forum Baseline Requirements
	MS ISO/IEC 14533 – Long-term non-repudiation
Data Governance And Integrity	ISO/IEC 38505 – Governance of Data
	ISO/IEC 30105 – IT-Enabled Services Lifecycle Processes
	ISO/IEC 25012 – Data Quality Model
	ISO/IEC 24028 – AI Trustworthiness
	OECD Principles on Data Governance and Privacy
	Malaysia's National Data Sharing Policy
Emerging Areas – Ai, Ethics, And Digital Resilience	ISO/IEC 23894 – AI Risk Management
	ISO/IEC 42001 – AI Management System Standard (new)
	NIST AI Risk Management Framework (AI RMF)
	IEEE 7000 Series – Standards for Ethical AI Design
	BS 31111 – Digital Resilience

Endnotes

Ang, Z., Cheah, K., Shakirah, M., Fun, W., Anis-Syakira, J., Kong, Y., & Sararaks, S. (2021). Malaysia's health systems response to covid-19. International Journal of Environmental Research and Public Health, 18(21), 11109. https://doi.org/10.3390/ijerph182111109

Anuar, S., Mokhtar, N., & Set, K. (2019). Teachers' behavior toward digital education. Journal of Information System and Technology Management, 32-47. https://doi.org/10.35631/10.35631/jistm.413004

Amin, M., A. (n.d.). Use digital space to improve education sector. Institut Masa. https://institutmasa.com/use-digital-space-to-improve-education-sector/

Blueprint to help Malaysia achieve digital economy aspirations. (n.d.). MIDA | Malaysian Investment Development Authority. https://www.mida.gov.my/mida-news/blueprint-to-help-malaysia-achieve-digital-economy-aspirations/

Beed. (2024, January 1st). Malaysian new education. Beed Blog. https://blog.beed.world/malaysian-new-education/

Build digital trust as foundation to address evolving cyber threats. (2024, August 7). The Sun. https://thesun.my/local-news/build-digital-trust-as-foundation-to-address-evolving-cyber-threats-gobind-AJ12825894 [1] https://www.isms.online/information-security/the-intersection-of-digital-trust-and-regulatory-compliance/

Build Digital Trust to as foundation to address evolving cyber threats-Gobind. (2024, August 7). Bernama. BERNAMA - Build digital trust as foundation to address evolving cyber threats - Gobind

Cetin, M. B. (2024). Evaluating the Effects of Digital Privacy Regulations on User Trust. arXiv preprint arXiv:2409.02614.

CyberSecurity Malaysia. (2024, August 6). CyberSecurity Malaysia Confers National Awards to Cyber Security Industry Leaders; Calls to Strengthen Malaysia's Digital Ecosystem through National Digital Trust Framework [Press release]. CyberSecurity Malaysia. https://www.cybersecurity.my/data/content_files/44/2609.pdf

Digital Trust Model For Digital Prosperity. (n.d.). Publication of PIKOM. Retrieved October 6, 2024, from https://www.pikom.org.my/DigitalTrustModel/Digital_TRUST_Model.pdf

Disterer, G. (2013). Iso/iec 27000, 27001 and 27002 for information security management. Journal of Information Security, 04(02), 92-100. https://doi.org/10.4236/jis.2013.42011

Gcaza, N., Solms, R., Grobler, M., & Vuuren, J. (2017). A general morphological analysis: delineating a cyber-security culture. Information and Computer Security, 25(3), 259-278. https://doi.org/10.1108/ics-12-2015-0046

Govt launches RM1.8b Malaysia Cyber Security Strategy. (2020, October 12). Malay Mail. https://www.malaymail.com/news/malaysia/2020/10/12/govt-launches-rm1.8b-malaysia-cyber-security-strategy/1912008

Lee, S. (2024, October 4). Building Digital Trust in Malaysia: Essential Steps Every Organisation Should Take. Cyber Security Asean; Cyber Security Asia. https://cybersecurityasia.net/building-digital-trust-in-malaysia/

Lee, C. (2002). Telecommunications reforms in malaysia. Annals of Public and Cooperative Economics, 73(4), 521-540. https://doi.org/10.1111/1467-8292.00203

Mohamed, N. (2023). Regulating online news portals in the era of ir 4.0 – should malaysia consider self-regulation?. Russian Law Journal, 11(4s). https://doi.org/10.52783/rlj.v11i4s.861

Nawang, N., Mohamed, A., & Mustaffa, A. (2020). Online news portals in malaysia - a revisit of the regulatory regime governing the media in the era of media convergence. Uum Journal of Legal Studies, 11. https://doi.org/10.32890/uumjls.11.1.2020.8263

Malaysia's Commitment to Strengthen Digital Trust – OpenGov Asia. (2024, August 27). Opengovasia. https://opengovasia.com/2024/08/07/malaysias-commitment-to-strengthen-digital-trust/

Malaysia Boosts Research Collaboration With Russia To strengthen higher education Ties. (2024, August 7). Bernama. BERNAMA - Malaysia Boosts Research Collaboration With Russia To Strengthen Higher Education Ties.

Malaysian government inks strategic collaboration with Google. (n.d.). Channel Asia. https://www.channelasia.tech/article/1303105/malaysian-government-inks-strategic-collaboration-with-google.html

MyDIGITAL Progress Report 2021: Building A Dynamic Digital Economy By 2030. (2022). MyDIGITAL. https://www.mydigital.gov.my/mydigital-progress-report-2021-building-a-dynamic-digital-economy-by-2030/

MyDigital. (n.d.). INTAN Official Portal. https://www.intanbk.intan.my/iportal/en/civil-servant/national-agenda/mydigital

National Digital Identity (ID) Framework for Malaysia Public Consultation Report. (2020). https://www.mcmc.gov.my/skmmgovmy/media/General/pdf/Public-Consultation-Report_National_DI.pdf

Rahim, S. (2024). Comparative literature analysis of national security management from the global to malaysia. International Journal of Social Science Research, 12(2), 82. https://doi.org/10.5296/ijssr.v12i2.21866

Samsuddin, S., Shaffril, H., Mohamed, N., & Bolong, J. (2021). Into the unknown: do people in low literacy rate areas practise digital reading?. Malaysian Journal of Library & Information Science, 26(2), 23-36. https://doi.org/10.22452/mjlis.vol26no2.2

Sari, N. (2024). The effect of google classroom-assisted learning on the academic achievement of students. International Journal of Academic Research in Business and Social Sciences, 14(4). https://doi.org/10.6007/ijarbss/v14-i4/21165

Wu, W., Shi, K., Wu, C., & Liu, J. (2021). Research on the impact of information security certification and concealment on financial performance. Journal of Global Information Management, 30(3), 1-16. https://doi.org/10.4018/jgim.20220701.oa2

Wok, S. and Mohamed, S. (2017). Internet and social media in malaysia: development, challenges and potentials.. https://doi.org/10.5772/intechopen.68848

Yunos, Z., Ahmad, R., Suid, S., & Ismail, Z. (2010). Safeguarding Malaysia's critical national information infrastructure (cnii) against cyber terrorism: towards development of a policy framework.. https://doi.org/10.1109/isias.2010.5604182

ZahidulIslam, M., Mokhtar, K., Afandi, N., & Anzum, R. (2021). Regulating online broadcast media against offensive materials in malaysia. Indian Journal of Science and Technology, 14(15), 1233-1238. https://doi.org/10.17485/ijst/v14i15.595

Digital Watch (2024). Malaysia launches digital education policy to foster digital literacy in students. Digital Watch. https://dig.watch/updates/malaysia-launches-digital-education-policy-to-foster-digital-literacy-in-students

Gnaneswaran, D. (2019, June 19). Only 24% of Malaysian consumers trust organizations offering digital services to protect their personal data: Microsoft study. Microsoft News. https://news.microsoft.com/en-my/2019/06/19/only-24-malaysian-consumers-trust-organizations-offering-digital-services-to-protect-their-personal-data-microsoft-study/

Harper, R. (2023, April 3). The intersection of digital trust and regulatory compliance. ISMS.online. https://www.isms.online/information-security/the-intersection-of-digital-trust-and-regulatory-compliance/

Malay Mail. (2024, May 16). Digital learning: Govt aims to provide each student with a device, implementation in phases, says DPM Zahid. Malay Mail. https://www.malaymail.com/news/malaysia/2024/05/16/digital-learning-govt-aims-to-provide-each-student-with-a-device-implementation-in-phases-says-dpm-zahid/134727

Malaysian Investment Development Authority. (April, 2021). Malaysia's journey in the digital age. MIDA Highlights. https://www.mida.gov.my/malaysias-journey-in-the-digital-age/

Nasarudin, N., H. (2024). Majority of Teachers, Students Ready for Digital Education. Bernama. https://www.bernama.com/en/news.php?id=2298043

Persatuan Industri Komputer Dan Multimedia Malaysia PIKOM (2024). Digital TRUST Model for Digital Prosperity (V1.0). http://www.pikom.org.my/DigitalTrustModel/Digital_TRUST_Model.pdf

Sharon, A. (2024, August 7). Malaysia's commitment to strengthen digital trust. OpenGov Asia. https://opengovasia.com/2024/08/07/malaysias-commitment-to-strengthen-digital-trust/ 28

Shields, G. (2023, December 28). Supporting privacy, security, and digital trust through effective enterprise data management programs. ISACA Now Blog. https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2023/supporting-privacy-security-and-digital-trust-through-effective-enterprise-data-management-programs

Siddharta, A. (2022, October 5). Trust in social media news in Malaysia 2019, by age group. Statista. https://www.statista.com/statistics/983048/malaysia-trust-in-social-media-news-by-age/

Zulkifli, F., & Zainal Abidin, R. (2024). Identity in the Digital Age: An Investigation of Malaysian Perspectives on Technology and Privacy. Journal of Advanced Research in Applied Sciences and Engineering Technology, 43(2), 1–20. https://doi.org/10.37934/araset.43.2.120

PIKOM. (2024). *PIKOM Cybersecurity Report*. http://www.pikom.org.my/2024/FOCS/PIKOM_Cybersecurity_Report.pdf

PIKOM. (2024). *Digital Trust Model*. http://www.pikom.org.my/DigitalTrustModel/Digital_TRUST_Model.pdf

Council of Europe. (2024). *Malaysia*. https://www.coe.int/en/web/octopus/-/malaysia

National Cyber Security Agency Malaysia. (2024). *Cyber Security Act, Regulations and Directives*. https://www.nacsa.gov.my

Ministry of Digital. (2024). *Trust and Security in the Digital Era*. https://digital.gov.my/en-GB/siaran/Trust-and-Security-in-The-Digital-Era

National Security Council Malaysia. (2020). *Malaysia cybersecurity strategy 2020-2024*. https://asset.mkn.gov.my/wp-content/uploads/2020/10/MalaysiaCyberSecurityStrategy2020-2024.pdf

DigiWorld. (2020, October 12). *Malaysia Cybersecurity Strategy*. https://dig.watch/resource/malaysia-cybersecurity-strategy

U.S. Department of Commerce. (2021, April 28). *Malaysia Cybersecurity*. https://www.trade.gov/market-intelligence/malaysia-cybersecurity

Ricoh Malaysia. (2023, January 11). *5 Pillars of Malaysia Cybersecurity Strategy 2020-2024*. https://www.ricoh.com.my/blogs/5-pillars-of-malaysia-cyber-security-strategy-2020-2024

The Edge Malaysia. (2023, October 17). *Issues: Rising threats, slow progress: The challenges in digital defence*. https://theedgemalaysia.com/node/701937

Yahoo News. (2023, October 18). *Digital Trust isn't just about Technology*. https://malaysia.news.yahoo.com/digital-trust-isn-t-just-151048165.html

The Malaysian Reserve. (2023, November 24). *Malaysia Launches Cybersecurity Strategy amidst Growing Threats*. https://themalaysianreserve.com/2023/11/24/malaysia-launches-cybersecurity-strategy-amids-growing-threats/

Free Malaysia Today. (2024, January 16). *Stronger Defense Needed Against Cybersecurity Threats*. https://www.freemalaysiatoday.com/category/highlight/2024/01/16/stronger-defence-needed-against-cybersecurity-threats

Al-Hawamleh, A. (2024). Examining the complex dynamics of cybersecurity practices and their influence on the quality of e-government services: evidence from the Kingdom of Saudi Arabia. Digital Policy Regulation and Governance, Volume 26, Issue 3, Pages 317-336. https://doi.org/10.1108/dprg-11-2023-0168

AllahRakha, N. (2024). Constitutional Safeguards for Digital Rights and Privacy. Irshad J. Law and Policy, 2(4), 31-43. https://doi.org/10.59022/ijlp.172

Alshehadeh, A. R., Al-Zaqeba, M. A. A., Elrefae, G. A., Al-Khawaja, H. A., & Aljawarneh, N. M. (2024). The effect of digital zakat and accounting on corporate sustainability through

financial transparency. Asian Economic and Financial Review, 14(3), 228-249. https://doi.org/10.55493/5002.v14i3.5016

Ashfaq, E. (2024). Zero trust security paradigm: a comprehensive survey and research analysis. jes, 19(2), 28-37. https://doi.org/10.52783/jes.688

Bansal, P. (2024). India's digital transformation: prospects and obstacles in the digital economy. International Journal of Economic Policy, Volume 4, Issue 2, Pages 53-57. https://doi.org/10.47941/ijecop.1947

Botha-Badenhorst, D. (2023). Exploring the convergence of innovation and cybersecurity: a framework. ecrm, 22(1), 18-25. https://doi.org/10.34190/ecrm.22.1.1490

Daah, C. (2024). Enhancing zero trust models in the financial industry through blockchain integration: a proposed framework. Electronics, 13(5), 865. https://doi.org/10.3390/electronics13050865

El-Maksoud, R. (2024). Investigating the significance of cybersecurity in building digital trust among Egyptian travel businesses. Journal of the Association of Arab Universities for Tourism and Hospitality, 26(1), 185-204. https://doi.org/10.21608/jaauth.2024.269299.1553

Frandell, A. and Feeney, M. (2022). Cybersecurity threats in local government: a sociotechnical perspective. The American Review of Public Administration, 52(8), 558-572. https://doi.org/10.1177/02750740221125432

Gupta, V. (2024). Consumer Trust in Digital Banking: A Qualitative Study of Legal and Regulatory Impacts. ISSLP, 3(2), 18-24. https://doi.org/10.61838/kman.isslp.3.2.4

Haque, A., Islam, A., Hyrynsalmi, S., Naqvi, B., & Smolander, K. (2021). Gdpr compliant blockchains–a systematic literature review. Ieee Access, 9, 50593-50606. https://doi.org/10.1109/access.2021.3069877

Hassan, A. (2024). Cybersecurity in banking: a global perspective with a focus on Nigerian practices. Computer Science & It Research Journal, 5(1), 41-59. https://doi.org/10.51594/csitrj.v5i1.701

He, Y., Huang, D., Chen, L., Ni, Y., & Ma, X. (2022). A survey on zero trust architecture: challenges and future trends. Wireless Communications and Mobile Computing, 2022, 1-13. https://doi.org/10.1155/2022/6476274

ISACA. (2024). State of Digital Trust 2024. Retrieved from https://www.isaca.org/resources/reports/state-of-digital-trust-2024 47

Lande Omorinsola Bibire Seyi, Oluwabunmi Layode, Henry Nwapali Ndidi Naiho, Gbenga Sheriff Adeleke, Ezekiel Onyekachukwu Udeh, Talabi Temitope Labake & Ebunoluwa Johnson (2024). Circular economy and cybersecurity: safeguarding information and resources in sustainable business models. Finance &Amp; Accounting Research Journal, 6(6), 953-977. https://doi.org/10.51594/farj.v6i6.1214

Liu, W. (2019). Modeling ransomware spreading by a dynamic node-level method. Ieee Access, 7, 142224-142232. https://doi.org/10.1109/access.2019.2941021

Kim, M., Lee, S., & Oh, C. (2021). Evaluating the trade-offs between development and conservation: a case study of land use change in a national park in Korea. Land, Volume 10, Issue 2, Page 152. https://doi.org/10.3390/land10020152

Kulova, M. (2020). Confidence and safety in the digital economy. https://doi.org/10.2991/fred-19.2020.55

Mateus-Coelho, N. (2023). Editorial - ARIS - Advanced Research in Information Security. Aris2 - Advanced Research on Information Systems Security, Volume 3, Issue 2, Pages 1-3. https://doi.org/10.56394/aris2.v3i2.33

Muravskyi, V. and Шевчук, О. (2021). Classification of stakeholders (users) of accounting information for the enterprise cybersecurity purposes. Herald of Economics, (1(99)), 83-96. https://doi.org/10.35774/visnyk2021.01.083

Nafees, M. (2023). Cybersecurity and privacy confidence in digital data: traversing the digital trust environment. https://doi.org/10.52458/9789388996747.nsp2023.eb.ch-14

Norbu, T., Park, J. Y., Wong, K. W., & Cui, H. (2024). Factors affecting trust and acceptance for blockchain adoption in digital payment systems: a systematic review. Future Internet, 16(3), 106. https://doi.org/10.3390/fi16030106

Paul, B. and Rao, M. (2022). Zero-trust model for smart manufacturing industry. Applied Sciences, 13(1), 221. https://doi.org/10.3390/app13010221

Poleto, T., Silva, M., Clemente, T., Gusmão, A., Araújo, A., & Costa, A. (2021). A suggestion for a risk assessment methodology utilizing bow-tie analysis for the sharing of medical image diagnoses in telemedicine. Sensors, 21(7), 2426. https://doi.org/10.3390/s21072426

Portela, D., Nogueira-Leite, D., Almeida, R., & Cruz-Correia, R. (2023). Economic ramifications of a cyberattack on a hospital inside a national health system: a descriptive case study. Jmir Formative Research, Volume 7, Article e41738. https://doi.org/10.2196/41738

Portes, A., N'Goala, G., & Cases, A. (2020). Digital transparency: dimensions, antecedents and consequences on the quality of customer relationships. Recherche Et Applications en Marketing (English Edition), 35(4), 72-98. https://doi.org/10.1177/2051570720973548

Shah, S. (2024). Trust as a factor influencing social wellbeing in the digital economy. Social Network Analysis and Mining, Volume 14, Issue 1. https://doi.org/10.1007/s13278-024-01238-5

Vasiu, I. & Vasiu, L. (2018). Cybersecurity as a crucial component of sustainable economic development. European Journal of Sustainable Development, Volume 7, Issue 4. https://doi.org/10.14207/ejsd.2018.v7n4p171 48

World Economic Forum. (n.d.). Digital Trust Framework. Retrieved from https://initiatives.weforum.org/digital-trust/framework

Yakel, E. (2024). An empirical examination of data reuser trust in a digital repository. Journal of the Association for Information Science and Technology, 75(8), 898-915. https://doi.org/10.1002/asi.24933

Alharbi, F. (2021). The use of digital healthcare platforms during the COVID-19 pandemic: the

consumer perspective. Acta Informatica Medica, 29(1), 51.

https://doi.org/10.5455/aim.2021.29.51-58

Boateng, K. A., Boateng-Coffie, R., & Darko, P. (2022). Trust in E-government Practices: A Platform Perspective of a Postal Service Organisation. The Asian Journal of Technology Management, 15(3), 235-255. https://doi.org/10.12695/ajtm.2022.15.3.4

Buechner, J. (2020). A revision of the buechner–tavani model of digital trust and a philosophical problem it raises for social robotics. Information, 11(1), 48. https://doi.org/10.3390/info11010048

Bunker, D. (2020). Who do you trust? the digital destruction of shared situational awareness and the COVID-19 infodemic. International Journal of Information Management, 55, 102201. https://doi.org/10.1016/j.ijinfomgt.2020.102201

Kye, B. and Hwang, S. (2020). Social trust in the midst of pandemic crisis: implications from covid-19 of South Korea. Research in Social Stratification and Mobility, 68, 100523. https://doi.org/10.1016/j.rssm.2020.100523

Marcellis-Warin, N., Marty, F., Thelisson, E., & Warin, T. (2022). Artificial intelligence and consumer manipulations: from consumer's counter algorithms to firm's self-regulation tools. Ai and Ethics, 2(2), 259-268. https://doi.org/10.1007/s43681-022-00149-5

Norbu, T., Park, J. Y., Wong, K. W., & Cui, H. (2024). Factors affecting trust and acceptance for blockchain adoption in digital payment systems: a systematic review. Future Internet, 16(3), 106. https://doi.org/10.3390/fi16030106

Ototsky, P., Manenkov, S., & Smoliak, A. (2022). Requisite trust requirements for digital society development. Kybernetes, 52(9), 2958-2975. https://doi.org/10.1108/k-04-2022-0610

Rebiazina, V. and Tunkevichus, E. O. (2022). Consumer digital trust: the main trends and research directions. Russian Management Journal, 19(4), 429-450. https://doi.org/10.21638/spbu18.2021.403

Ting, H. L. J., Kang, X., Li, T., Wang, H., & Chu, C. (2021). On the trust and trust modeling for the future fully-connected digital world: a comprehensive study. IEEE Access, 9, 106743-106783. https://doi.org/10.1109/access.2021.3100767

Ward, P., Miller, E., Pearce, A., & Meyer, S. (2016). Predictors and extent of institutional trust in government, banks, the media and religious organisations: evidence from cross-sectional surveys in six asia-pacific countries. Plos One, 11(10), e0164096. https://doi.org/10.1371/journal.pone.0164096

Yakel, E. (2024). An empirical examination of data reuser trust in a digital repository. Journal of the Association for Information Science and Technology, 75(8), 898-915. https://doi.org/10.1002/asi.24933

Zhghenti, T. and Chkareuli, V. (2021). Enhancing online business sector: digital trust formation process. Marketing and Management of Innovations, 5(2), 87-93. https://doi.org/10.21272/mmi.2021.2-07

Aavik, G. and Krimmer, R. (2016). Integrating digital migrants: solutions for cross-border identification from e-residency to Eidas. A case study from Estonia., 151-163. https://doi.org/10.1007/978-3-319-44421-5_12

Chohan, S. and Hu, G. (2020). Success factors influencing citizens' adoption of IoT service orchestration for public value creation in smart government. Ieee Access, 8, 208427-208448. https://doi.org/10.1109/access.2020.3036054

Cvjetković, S., Stojković, V., Mandić-Rajčević, S., Matovic-Miljanovic, S., Janković, J., Vranes, A., … & Stamenković, Ž. (2022). Societal trust related to COVID-19 vaccination: evidence from western Balkans. Sustainability, 14(20), 13547. https://doi.org/10.3390/su142013547

Hartanti, F., Abawajy, J., Chowdhury, M., & Shalannanda, W. (2021). Citizens' trust measurement in smart government services. Ieee Access, 9, 150663-150676. https://doi.org/10.1109/access.2021.3124206

Kulova, M. (2020). Trust and security in the digital economy. https://doi.org/10.2991/fred-19.2020.55

Kumar, A., Malik, A., Batra, I., Ahmad, N., & Johar, S. (2022). Digital society social interactions and trust analysis model. Peerj Computer Science, 8, e1129. https://doi.org/10.7717/peerj-cs.1129

Norbu, T., Park, J. Y., Wong, K. W., & Cui, H. (2024). Factors affecting trust and acceptance for blockchain adoption in digital payment systems: a systematic review. Future Internet, 16(3), 106. https://doi.org/10.3390/fi16030106

Ototsky, P., Manenkov, S., & Smoliak, A. (2022). Requisite trust requirements for digital society development. Kybernetes, 52(9), 2958-2975. https://doi.org/10.1108/k-04-2022-0610

Saeed, A. and Riaz, H. (2021). Navigating through firm–environmental groups' relationships: the impact of societal trust on corporate environmental strategy. Business Strategy and the Environment, 30(8), 3552-3568. https://doi.org/10.1002/bse.2819

Shah, S. (2024). Trust as a determinant of social welfare in the digital economy. Social Network Analysis and Mining, 14(1). https://doi.org/10.1007/s13278-024-01238-5

Toth, I., Heinänen, S., & Blomqvist, K. (2020). Freelancing on digital work platforms – roles of virtual community trust and work engagement on person-job fit. Vine Journal of Information and Knowledge Management Systems, 50(4), 553-567. https://doi.org/10.1108/vjikms-12-2018-0124

CyberSecurity MALAYSIA

Address

CyberSecurity Malaysia,

Level 7 Tower 1, Menara Cyber Axis,

Jalan Impact,

63000 Cyberjaya,

Selangor Darul Ehsan, Malaysia.

Phone : +603-8800 7999

Fax : +603-8008 7000

Email : digitaltrust@cybersecurity.my