ISSN 2228-9860 eISSN 1906-9642 CODEN: ITJEA8

International Transaction Journal of Engineering, Management, & Applied Sciences & Technologies

http://TuEngr.com

Modeling a Digital Trust Framework to Address Cybersecurity Issues in Malaysia's Digital Economy

Aumuhaimi Md. Yusof[1], Muhamad Khairulnizam Zaini[2*], Irni Eliana Khairuddin[2], and Noraáyu Ahmad Uzir[2]

[1]Royal Malaysian Customs Department, Putrajaya, MALAYSIA.
[2]Faculty of Information Management, Universiti Teknologi MARA, 40150 Shah Alam, Selangor, MALAYSIA.
**Corresponding Author (Tel: +603 7962 2173, Email: nizam0374 @uitm.edu.my)*

Paper ID: 15A4B

Volume 15 Issue 4

Received 23 March 2023
Received in revised form 19 October 2023
Accepted 26 October 2023
Available online 24 June 2024

Keywords:
Cybersecurity; Digital Economy; Digital Trust, Data security; Cyber threats; Cybercrimes; Digital businesses; Data privacy; Cybersecurity challenges; Security risk management.

Abstract

Embracing the concepts of cybersecurity in the digital economy is critical for overcoming security concerns in this new economic era. This article provides a review of significant work on cybersecurity and its technology, especially in the digital economy, and critically analyses its usefulness in understanding how it may overcome certain challenges in the ecosystems of the digital economy. Several advantages and limitations of current cyber-related trust models and theories are identified, and a conceptual framework for research on ways to explore some specific cybersecurity challenges raised by the digital economy's ecosystems, as well as how a digital trust model could address such challenges, is proposed and discussed.

Discipline: Information Science & Cybersecurity, Digital Economy.

Cite This Article:

Md Yusof, A., Zaini, M. K., Khairuddin, I. E., and Ahmad Uzir, N. (2024). Modeling a Digital Trust Framework to Address Cybersecurity Issues in Malaysia's Digital Economy. *International Transaction Journal of Engineering, Management, & Applied Sciences & Technologies, 15*(4), 15A4B, 1-12. http://TUENGR.COM/V15/15A4B.pdf DOI: 10.14456/ITJEMAST.2024.21

1 Introduction

The term "digital economy" refers to a wide variety of economic activities that rely on digitized information and knowledge as major inputs of production. According to World Bank Group (2019), the digital economy increased at a rate of 9% per year from 2010 in terms of value-added and is predicted to account for 20% of the GDP by 2022. For Malaysia, the digital economy is continuously expected to grow in years to come. The digital economy, which is built on the

application of disruptive technology to new business models and the delivery of goods and services in a viable manner, offers an excellent potential for businesses of all sizes. In addition, the interconnected capabilities of disruptive technologies are enablers for the digital economy and provide many advantages.

The successful development of the digital economy will be ensured by strengthening various economic elements in accordance with the latest technologies. Basically, the digital economy (as an ecosystem) includes a combination of digital infrastructure, in no-diversification information, and communication technologies for doing business (Chernyakov & Chernyakova, 2018). Although the evolving digital economy, related innovations, and emerging technologies present substantial opportunities for economic growth and enhanced societal benefits, they are unfortunately vulnerable to trust-related risks. In this context, many countries (especially developing countries) are not equipped to handle the risks associated with the heavy reliance on core digital infrastructure, strategic systems, strategic data, and related policies to promote trust (Hanna, 2020). The continual growth of digital incidents and threats to economic and social activities with much more sophistication and greater consequences has manifested the issues globally. To thrive, the digital economy requires strong cybersecurity risk management and privacy protection. Consequently, to establish trust in the digital economy, it is important to address the digital security and privacy threats as economic and societal problems at the highest degree of priority (Economist, 2018).

While most of the work on cybersecurity has centered on social and economic losses to individuals and organizations, slight attention has been paid to the impact of Malaysian businesses being exposed to high levels of cyber-attacks, particularly those related to the digital economy. The lack of interest in this study suggests that cyber security management in this new age economy is unexplored and needs to be investigated further. The objective of this paper is to explore the comprehensive landscape of cyber security management in Malaysia's business context. This paper discusses the cybersecurity challenges and offers a review of relevant work on trust in the digital economy ecosystem, and critically examines its value in understanding the issues of cybersecurity in that area, and how to mitigate them. The main contribution of this paper is the development of a conceptual research framework to explore the specific trust challenges raised by cybersecurity threats.

2 Literature Review

The progression of the digital economy is mainly focusing on the integration of digital technology and traditional economic activities. As a result, it is powered by substantial technological innovation, pro-growth government policies, and a high capacity for digital entrepreneurship. Globally, the trend of economic growth in the digital economy is essentially linked to the emergence of new ICTs, such as embedded sensors in objects, advanced end-user devices, novel business models and platforms, digital services, and automation and robotics

technologies. However, the high dependence on the use of ICTs in the economic sphere has the potential to vulnerably increase the array of cyber threats. Mining on past literature, some of the issues found that are related to the digital economy and cybersecurity are discussed in the next section.

2.1 Data Security and Privacy Issues

Data and platforms are recognized as important drivers for the digital economy (Liu et al., 2021). Commercial, and societal interactions in this networked world have generated an incredible number of detailed machine-readable data. Utilization of data created from the digital footprints is vital and offers an opportunity to transform it into useful information for better decision-making and agility. In this spectrum, these digital ecosystems tend to have the potential to serve as a platform for both business and government and act as data miners gathering information about every element of user activity, behavior, and lifestyle inside these ecosystems. Access to data is increasingly critical. For businesses, data seems to be vital for decision-making, production, transaction, and relationship management for their agility (Zaini et al., 2020). In fact, in the digital economy, data can be monetized in different ways such as through advertisement and other services like transactions, product optimizations, and other digital services. It is obvious that data could create new knowledge sources, innovations, and profits if it is efficiently examined and turned into intelligence. However, the use of personal data might contradict the privacy expectations of customers (Carpenter et al., 2016). Hence, in a data-driven economy, it is obvious that data and privacy are two key competitive aspects. It is apparent that the crucial needs for data and the right to privacy seem to be conflicting in the digital ecosystems. In other words, the capacity to apply extensive data collection using cutting-edge technology in digital ecosystems has sparked a skeptical view that data privacy and security are about to vanish, creating excessively stringent limitations that curb effective production, trade, and innovations in the ecosystem. Therefore, to strengthen the trustworthiness of the digital economy, the growth and utilization of its ecosystems must be accompanied by privacy and protection of the data (Rosadi, 2018).

2.2 Malware Attacks on eCommerce Platforms

The global growth of malware has increased threats and hazards in cyberspace. The use of mobile devices in the digital economy is also prevalent and prone to be affected by the growth of malware. This is particularly alarming as the fast growth of technology makes mobile devices more useful and easier, particularly benefiting economic sectors. As reported in Digital 2019 for Malaysia's eCommerce activities, 58% of citizens had made an online purchase via a mobile device while 44% of citizens had chosen a laptop or desktop computer to complete an online purchase. The increasing use of mobile devices to access eCommerce platforms has raised the risk of cyber-attacks. Research has shown that data breaches caused by vulnerabilities in mobile devices and e-commerce applications could have suffered losses in the hundreds of millions of dollars globally (Zimba et al, 2019). The infiltrations of eCommerce platforms by Malware are also apparent. In

many cases, malware not only reacts as a harmful application in online transactions but is also used to carry out sabotage activities in the digital economy. The ability of malware to drill into a closed network leads to a sense of mistrust in eCommerce activities. These assertions are being debated and will have an influence on the expansion of Malaysia's digital economy as they place a low level of trust in the digital economy.

2.3 Insecure Internet

The Internet's security concerns were formerly limited to preventing physical breakdowns, rather than more complicated challenges of today's concerns such as identification and data veracity, hyperconnectivity brought on by the Internet of Things (IoT), and growing digital fragmentation. Instead, the Internet was created to allow for high degrees of anonymity, data sharing, and redundancy which then need a trust basis. However, the growth of new networked and digital technologies has resulted in a significant rise in crime speed, distance over which it may be perpetrated, and volume (Wall, 2015). Many of the difficulties confronting the Internet today are a result of its explosive expansion in both user and application aspects. Over the last several years, the Internet's evolution has shifted from a scientific to a platform that allows a new generation of businesses (Duah & Kwabena, 2015). The Internet now underpins the whole digital economy. Simultaneously, as organizations, individuals, and communities become more interconnected, those relationships are getting more complicated. A single breach can have significant, cascading consequences if the Internet does not become more reliable and trustworthy. It is also crucial to understand that the structure of the Internet's geographical and political boundaries is irrelevant, as criminals may originate assaults from anywhere in the globe and execute them wherever they see fit (Ibrahim, 2019). As a result of the borderless digital world, it will be difficult to solve crime and bring justice to the victims and could be a major hindrance to successful digital businesses. Hence, to promote the expansion of Malaysia's digital economy, creating trust in Internet safety and its governance is a vital factor to be considered.

2.4 Cybersecurity Concerns are as much Psychological as they are Technological

Mind games and exploits of human psychology, emotions, and errors are now apparent as parts of cybercriminal games. The use of psychological manipulation to persuade someone to reveal sensitive information is increasingly reported in security incidents. Socially engineered attacks, online frauds, business email compromises, identity-related crimes, and other similar assaults are just a few examples of possible mind hacking cybercriminals may perpetrate using technology (Nurse, 2018). This indicates that cybercriminals are not only interested in hacking into technology but at the same time, psychology as well. Technology has allowed old crimes to be committed through a new medium (McDaniels, 2018). The interconnectedness of digital ecosystems, along with millions of devices connected has created avenues for cybercriminals to find the right candidates to victimize. Cybercriminals are profound in their ways of continuously seeking new

vulnerabilities in the systems. Often, humans are always targeted for their weaknesses in this context (Arora, 2016). For cybercriminals, mind games could offer them tremendous rewards. In many cases, the goal is to exploit human weaknesses such as greed, naiveté, and ignorance. Online fraud or forgery does exist in many possible ways and in many cases, victims are tricked using digital technologies. Particularly, attacks such as ransomware have become more severe in the digital economy due to the advent of cryptocurrencies and the application of IoT in the ecosystems (Srinivasan, 2017; Muslim et al., 2019). Ransomware involves the human psychology of fear and insatiability exploited by the attackers. According to Trendmicro (2016), fear has remained the biggest factor for the success of ransomware attacks. In this case, the understanding of the victim's psyche especially in the digital ecosystem has largely contributed to its effectiveness.

Apparently, businesses are at a very real danger of cybersecurity threats in the digital economy's ecosystems. Cyberthreats are inevitable no matter how sophisticated the technologies are adopted to work in the ecosystems. As ever, some of those threats are evolving to keep pace and sometimes stay ahead of the changing IT landscape in the business environment. Figure 1 summarizes the above discussions.

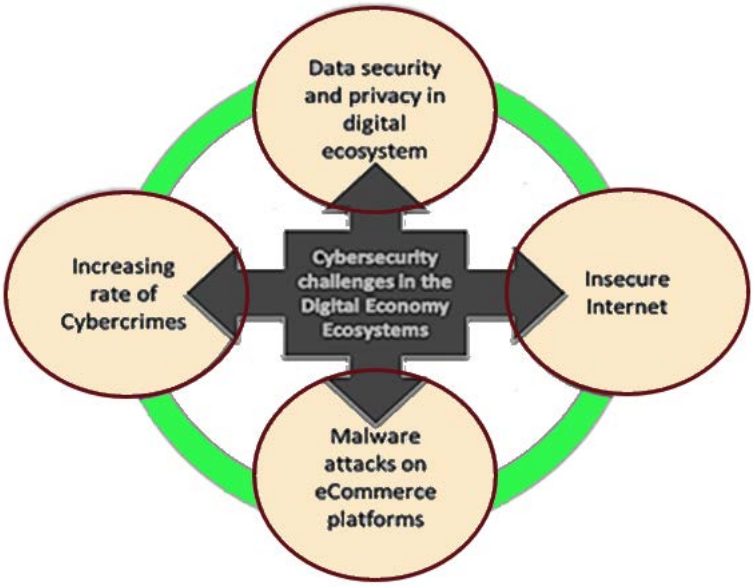

Figure 1: Depiction of Cybersecurity challenges in the Digital Economy ecosystems.

3 The Conceptual Framework

3.1 Overcoming Cybersecurity Challenges in the Digital Economy: The Proposed Framework

Businesses are increasingly vulnerable to cybersecurity risks as they accelerate digital transformation initiatives. This scenario suggests that protecting and safeguarding businesses, consumer data, and brand reputation from cyber threats and cybercriminals is serious business. Proactive cyber defense especially in the digital economy's ecosystems is now paramount and essential for the successful implementation of the digital economy. New mechanisms to boost business, risk management, and compliance, specifically those cyber-related issues are exceptionally essential. The next section discusses this further.

3.2 The Future of Digital Trust

In general, trust has become the key determinant in facilitating electronic transactions and is a key instrument to connect individuals, businesses, and institutions in the digital economy's ecosystems. Beyond that, trust is also imperative to mitigate cybersecurity challenges in that context. The future of digital trust is shaped by a vast variety of antecedents. In several studies, the factors associated with the development of the future of digital trust for cybersecurity and the digital economy are grouped into different categories which are social, technological, economic, political, and legal forces.

Generally, cybersecurity is a multi-dimensional concept where all the different perspectives should be considered. In a bigger picture, it encompasses economic and social prosperity, technology, national, and international security, as well as cyber law enforcement. Among all the cybersecurity dimensions related to the digital economy, the technology element will be the research framework's spotlight within this study.

Zaini et al. (2020) claims that components such as logical controls utilizing technology resources to mitigate cybersecurity breaches are widely used in digital business environments. The technological-based mechanisms including encryption technologies to secure business are present in the study, specifically with concerns on the protection of IT infrastructures that provide access to valuable electronic data and information belonging to the organizations, thus indicating technological trust is core for digital businesses. Obviously, the technological controls to enhance the security posture of the digital ecosystem are highly important to build trust for digital businesses in such a digital ecosystem. Additionally, in technological cybersecurity dimensions, social trust related to security issues such as data security and privacy in the digital ecosystem is also deemed to be crucial. Having mechanisms to ensure the security of data and privacy is crucial to ensure such categories of beliefs can be sustained.

It is well known that the digital economy has a plethora of centralized data platforms that collect data from real-world economic activities using the Internet, IoT, AI, big data, and other recent technologies (Zhao et al., 2019; Chen, 2017). In the meantime, for the digital economy, issues related to mutual trust have centered on the development of a decentralized digital economy which is predicated on resolving the problem (Chen, 2017). The rise of new technologies such as blockchain has the potential to be the key pillar of trust management in decentralized settings by replacing trust in institutions with the end user's trust in technology (Ferrari & Thuraisingham, 2020). In line with that, Crossby et al. (2015) asserted that the blockchain's characteristics as a decentralized and pseudo-anonymous platform can pose important trust challenges to overcome the illicit use of tools and cyberattacks perhaps for the digital ecosystems. Furthermore, blockchain decentralization is expected to foster trust and importantly to bypass a potential dishonesty in such ecosystems (Sas & Khairuddin, 2017).

On the other side, Internet governance should not be overlooked mainly because it acts as the main platform for the digital economy. Kende (2020) in his study mentioned that as more activities are shifted online, the resilience of online activities becomes more apparent, and cybersecurity has become a critical issue. In a more global context, efforts to foster digital trust to improve internet usage as well as to prevent cyber-attacks have received a lot of attention from scholars and practitioners. To address these issues, national policies, and legislation with regard to Internet governance in the digital economy ecosystems is crucial.

Privacy and security breaches have undermined trust in digital products & services. This concern is obvious with trends of such incidents in the digital economy's activities. Reflecting the need to address this, many business organizations now recognize the need for digital trust. Many studies have looked at various aspects as contributions to digital trust in the digital economy including political, social, economic, law, and enforcement. However, not many studies especially in Malaysia have really investigated the technological aspects that would contribute towards strengthening the digital trust for mitigating cybersecurity challenges in the digital economy. Considering the core dimensions that IT holds in the digital economy's ecosystems, especially in technical and socio-economic terms, cybersecurity has become a fundamental need, highlighting the strategic & critical needs in planning, and implementing cybersecurity for the digital economy.

The studies of technological aspects for building digital trust to reduce cybersecurity challenges are imperative for Malaysia's business organizations to excel in the digital economy's ecosystems. This study will explore the technological aspects of cybersecurity that have potential contributions as antecedents for strengthening the digital trust elements in the digital economy. Figure 2 illustrates the framework of the study.

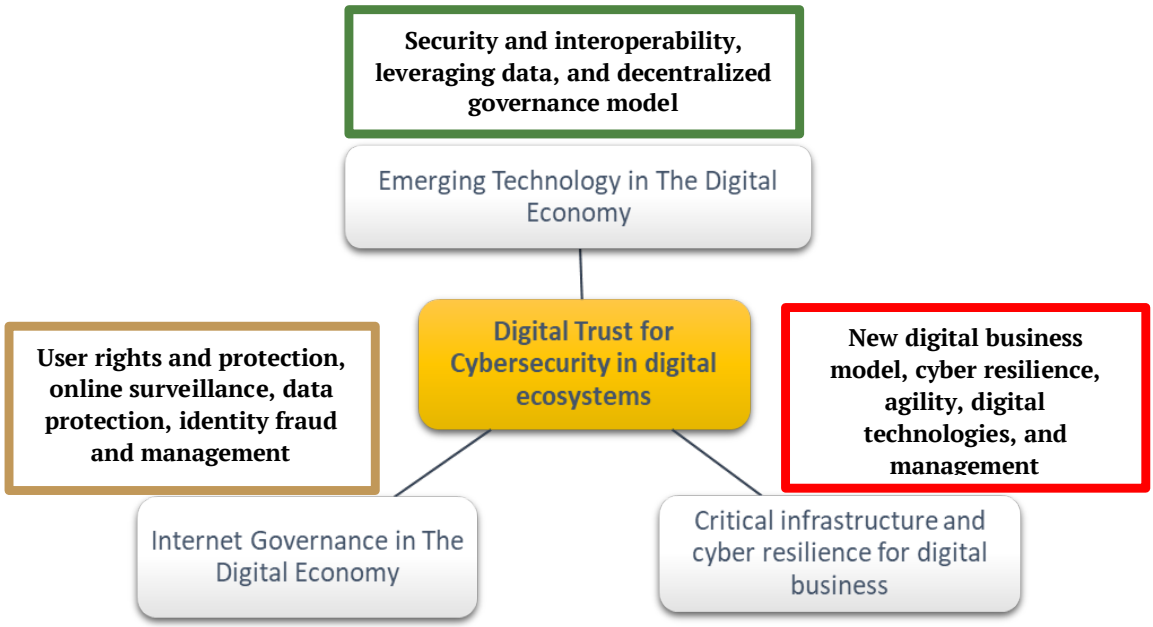

Figure 2: Proposed Framework for Mitigating Cybersecurity Challenges in the Digital Economy

3.2.1 Emerging Technology in the Digital Economy

Distributed ledger technology, namely blockchain, big data, artificial intelligence (AI), and cloud technologies are the important technologies that underpin financial transformations. However, rather than serving as a platform for the digital economy, these emerging technologies may serve as a turning point in the evolution of online transaction trust. The advent of new technologies such as blockchain is a cornerstone of trust management in decentralized settings and to restore trust in services (Ferrari & Thuraisingham, 2020; Khairuddin & Sas, 2019). Blockchain technology assures data integrity, anti-tampering, and traceability (Chen et al., 2019). Blockchain technology also offers extremely secure data in all areas utilizing encryption and a fingerprint that validates the data.

3.2.2 Internet Governance in the Digital Economy

It is known that the Internet is an ecosystem of technologies, protocols, hardware, software, and information, rather than a single system. Therefore, Internet governance should be a multi-stakeholder, including and considering the perspectives and requirements of the government, business sector, and civil society. Specifically, the government of Malaysia has taken cybercrime law practices seriously. To address crimes committed over the Internet, many legislative measures have been enacted, including the Computer Crime Act of 1997, the Communications and Multimedia Act of 1998 (CMA), the Malaysian Communications and Multimedia Commission Act of 1998, the Digital Signature Act of 1997, and the Electronic Transactions Act of 2006. In fact, all these Acts have been practiced in Malaysia towards the digitalization processes to protect user rights, prevent online crimes, protect data transmission, prevent fraud, and strengthen cyber resilience and identity management and many others. On a greater scale, multilateral collaboration is supposed to instill and maintain trust in digital security and privacy risk management. Such multilateral cooperation in good governance will establish the digital economy arrangement and cooperation to support the productivity and competitiveness of businesses, especially in developing a global framework and obligations that can enable secure digital trade with the use of Internet technologies (Malaysia Digital Economy Blueprint, 2021).

3.2.3 The Digital Enterprise and the New Digital Business Model for Security of Businesses

The ability to plan for, respond to, and recover from a cyber-attack will help decrease cyber risks. According to Peter (2017), prioritizing cyber resilience is critical, especially at public and regional/international policy levels. Moving forward to the digital transformation of the economic sector, Hathaway (2013) agreed that a high level of cyber resilience is required to ensure the trust of Internet transactions. This will be extended to include all business models that support the digital economy, such as business-to-business (B2B), business-to-consumer (B2C), and consumer-to-consumer (C2C). The digital economy trust shall be raised upon the security and cyber resilience

assurance as part of the new business model (Fortinet, 2019). Following that, security must be fully integrated into the broader technological environment to guarantee comprehensive visibility and control to better correlate data, and identify, and even predict both known and undiscovered threats. Finally, security must be automated and integrated across devices and applications to respond to attacks efficiently.

4 Research Implications

As the digital economy comes to the fore around the world, the likelihood of cybersecurity threats and attacks has also increased. With threats becoming increasingly sophisticated, the need to handle such threats has grown exponentially and requires strong focus. As for Malaysia, this effort is in alignment with the government to support the pervasive use of digital technology for the National Digital Economy Initiative (Digital Malaysia and MyDigital). This research is also aligned with the Ministry of Science and Technology of Malaysia (MOSTI) 10-10 Malaysia Science, Technology, Innovation and Economy (MySTIE) framework to pave the way for the nation to improve its innovative and creative capabilities as a means of enhancing economic competitiveness and quality of life by incorporating core technologies in business and financial services. Apart from that, it is aligned with Key Economic Growth Activities (KEGA 2) - Ekonomi Digital (Digital Economy), which eventually contributes to Sustainable Development Growth 8 (Decent Work and Economic Growth). As highlighted before, the study of the relationship between cybersecurity and digital trust in the digital economy has received little attention among researchers in this nation. As a result, the findings of this study will give empirical findings on the difficulties. The main contribution of this study is expected in the form of the establishment of an empirical-based framework. The findings of this study will provide empirical evidence on the critical aspect of cybersecurity management, tools, and technologies that would contribute towards building resilient business organizations in the façade of the new economy. This study aims to address the need for a detailed, coherent, and validated study to examine the requirements of a new and evolving cybersecurity technology for it to integrate into the digital trust framework for the digital economy.

5 Conclusion

In conclusion, a review and realistic framework for overcoming cybersecurity challenges in Malaysia's Digital Economy is provided in this paper. Particularly important, technology elements will be the theme of the study, and essentially, all the preceding in the framework will map to solve challenges that relate to 1) data security and privacy; 2) insecure and imperfection of the Internet, and cybercrimes; and 3) secured eCommerce platforms. Thus, in terms of future research, an extensive study shall be carried out to investigate the actual cybersecurity trust issues that exist in Malaysia's digital economy's ecosystems, as well as the technological elements that are best incorporated into the digital trust framework to mitigate cybersecurity challenges by conducting a qualitative approach. Furthermore, research is needed to validate the established framework to give

a trustworthy and useful model. Collaborative research is also required to better investigate the potential roles of emerging technologies in the digital economy. To obtain accurate and relevant data and responses for this research, practitioners' and governments' experiences in the digital economy must be included.

6 Acknowledgement

The authors would like to thank the Office of Deputy Vice-Chancellor (Research & Innovation) Universiti Teknologi MARA (UiTM) for the funding of this study under the research grant GPK 5/3/ (158/2020).

7 References

Arora, B. (2016). Exploring and analyzing Internet crimes and their behaviours. *Perspectives in Science*, 8, 540–542. DOI: 10.1016/j.pisc.2016.06.014

Carpenter, D., McLeod, A., Hicks, C., & Maasberg, M. (2016). Privacy and biometrics: An empirical examination of employee concerns. *Information Systems Frontiers*, 20(1), 91–110. DOI: 10.1007/s10796-016-9667-5

Chen, L., Lee, W. K., Chang, C. C., Choo, K. K. R., & Zhang, N. (2019). Blockchain-based searchable encryption for electronic health record sharing. *Future Generation Computer Systems*, 95, 420–429. DOI: 10.1016/j.future.2019.01.018

Chen, Y. (2017). Service-Oriented Computing and System Integration: Software, IoT, Big Data, and AI as Services. 6th Ed., Kendall Hunt Publishing.

Chernyakov, M., & Chernyakova, M. (2018). Technological Risks of the Digital Economy. *Journal of Corporate Finance Research*, 12(4), 99–109. DOI: 10.17323/j.jcfr.2073-0438.12.4.2018.99-109

Crosby, M., Nachiappan, P. P., Verma, S., & Kalyanaraman, V. (2015). BlockChain Technology. *Sutardja Center for Entrepreneurship & Technology Technical Report, 16*.

Duah, F. A., & Kwabena, A. M. (2015). The impact of cybercrime on the development of electronic business in Ghana. *European Journal of Business and Social Sciences*, 4(1), 22–34. http://www.ejbss.com

EPU. (2021). Malaysia Digital Economy Blueprint. https://www.epu.gov.my/sites/default/files/2021-02/malaysia-digital-economy-blueprint.pdf

Ferrari, E., & Thuraisingham, B. (2020). Digital Trust: Trust Management in Cyberspace. *IEEE Internet Computing*, 24(6), 6–7. DOI: 10.1109/mic.2020.3028898

Fortinet. (2019). Three Key Strategies for Securing Digital Business. Fortinet Blog. https://www.fortinet.com/blog/industry-trends/transforming-security-using-three-basic-principles

Hanna, N. K. (2020). Assessing the digital economy aims, frameworks, pilots, results, and lessons. *Journal of Innovation and Entrepreneurship*, 9(1). DOI: 10.1186/s13731-020-00129-1

Hathaway, M., Demchak, C., Kerben, J., McArdle, J., & Spidalieri, F. (2013). Cyber readiness index 1.0. Great Falls, VA: Hathaway Global Strategies LLC.

Ibrahim, U. (2020). The Impact of Cybercrime on The Nigerian Economy and Banking System.

https://ndic.gov.ng/wp-content/uploads/2020/08/NDIC-Quarterly-Vol-34-No-12-2019-Article-The-Impact-Of-Cybercrime-On-The-Nigerian-Economy-And-Banking-System.pdf

Kende, M. (2020). Internet governance in international Geneva: The observatory of the foundation pour Genève. http://www.graduateinstitute.ch/sites/internet/files/2020-09/FPG_Bulletin%20Internet%20Governance-DIGITAL.pdf

Liu, S., Huang, W. W., Lu, H., & Watson, R. (2021). PACIS 2019: Emerging technology, business, and application in digital economy. *Information & Management*, 58(6), 103466. DOI: 10.1016/j.im.2021.103466

McDaniel, B. (2018). An In-Depth Look into Cybercrime. *Themis Research Journal of Justice Studies and Forensic Science, 6*(1). DOI: 10.31979/themis.2018.0610

Muslim, A. K., Mohd Dzulkifli, D. Z., Nadhim, M. H., & Abdellah, R. H. (2019). A Study of Ransomware Attacks: Evolution and Prevention. *Journal of Social Transformation and Regional Development*, 1(1), 18–25. https://publisher.uthm.edu.my/ojs/index.php/jstard/article/view/5503

Nurse, Jason. (2018). Cybercrime and You: How Criminals Attack and the Human Factors That They Seek to Exploit. 10.1093/oxfordhb/9780198812746.013.35.

Peter, A. S. (2017). Cyber resilience preparedness of Africa's top-12 emerging economies. *International Journal of Critical Infrastructure Protection*, 17, 49–59. DOI: 10.1016/j.ijcip.2017.03.002

Rosadi, S. (2018). Protecting Privacy on Personal Data in Digital Economic Era: Legal Framework In Indonesia. *Brawijaya Law Journal*, 5(2), 143–157. DOI: 10.21776/ub.blj.2018.005.01.09

Sas, C., & Khairuddin, I.E. (2017). Design for Trust: An Exploration of the Challenges and Opportunities of Bitcoin Users. *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*.

Srinivasan, C. (2017). Hobby hackers to billion-dollar industry: the evolution of ransomware. *Computer Fraud & Security*, 2017(11), 7–9. DOI: 10.1016/s1361-3723(17)30081-7

The Economist. (2018). America should borrow from Europe's data-privacy law. https://www.economist.com/leaders/2018/04/05/america-should-borrow-from-europes-data-privacy-law

Trendmicro. (2016). Why Ransomware Works: The Psychology and Methods Used to Distribute, Infect, and Extort. Security News. https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/why-ransomware-works-psychology-and-methods-to-distribute-infect-and-extort

Wall, D. S. (2015). The Internet as a Conduit for Criminal Activity. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=740626

World Bank Group. (2019). *Malaysia's Digital Economy: A New Driver of Development 2019*. https://openknowledge.worldbank.org/bitstream/handle/10986/30383/129777.pdf

Zaini, M. K., Masrek, M. N., & Abdullah Sani, M. K. J. (2020). The impact of information security management practices on organisational agility. *Information & Computer Security*, *28*(5), 681–700. DOI: 10.1108/ics-02-2020-0020

Zhao, H., Cui, W., Li, S., & Xu, R. (2019). Token Economy: A New Form Economy with Decentralized

Mutual Trust and Collective Governance. *2019 IEEE 14th International Symposium on Autonomous Decentralized System (ISADS)*. DOI: 10.1109/isads45777.2019.9155592

Zimba, A., & Chishimba, M. (2019). On the Economic Impact of Crypto-ransomware Attacks: The State of the Art on Enterprise Systems. *European Journal for Security Research*, 4(1), 3–31. DOI: 10.1007/s41125-019-00039-8

Aumuhaimi is a PhD candidate at the Faculty of Information Management, Universiti Teknologi MARA (UiTM) Shah Alam, Malaysia. She is currently an IT Officer at the Royal Malaysian Customs Department, Putrajaya, MALAYSIA. She got a master's degree in Information Management from UiTM in 2021. Her research area is mainly on the Cybersecurity Management in Digital Economy.

Dr. Muhamad Khairulnizam is a Senior Lecturer at the Faculty of Information Management, Universiti Teknologi MARA (UiTM) Shah Alam, Malaysia. He got his PhD in Information Management from the Universiti Teknologi MARA (UiTM) Shah Alam, Malaysia. His research focuses on Cybersecurity Technology and Management.

Dr. Irni Eliana is a Senior Lecturer at the Faculty of Information Management, Universiti Teknologi MARA (UiTM) Shah Alam, Malaysia. She got her PhD in Computer Science from the Lancaster Universiti, United Kingdom. Her research focuses on Blockchain technology, Information Architecture and HCI.

Dr. Noraáyu is a Senior Lecturer at the Faculty of Information Management, Universiti Teknologi MARA (UiTM) Shah Alam, Malaysia. She got her PhD in Informatics from the University of Edinburgh, United Kingdom. Her research focuses on Learning Analytics.