


RESEARCH ARTICLE | JUNE 12 2023

Fundamental of zero trust among digital employees in migration to industry 4.0: Cyber security and movement to iot in Malaysian perspectives

Irza Hanie Abu Samah; Intan Maizura Abd Rashid ; Abdul Shukor Shamsudin; Wan Ahmad Fauzi Wan Husain; Mohammad Harith Amlus; Hariri Hamzah

 Check for updates

AIP Conference Proceedings 2608, 020041 (2023)

<https://doi.org/10.1063/5.0127923>


View
Online


Export
Citation

 CrossMark

AIP Advances

Why Publish With Us?

	25 DAYS average time to 1st decision		740+ DOWNLOADS average per article		INCLUSIVE scope
---	---	---	--	---	---------------------------

[Learn More](#)

 AIP
Publishing

Fundamental of Zero Trust Among Digital Employees in Migration to Industry 4.0: Cyber Security and Movement to IoT in Malaysian Perspectives

Irza Hanie Abu Samah^{1, 8}, Intan Maizura Abd Rashid^{2, 8, a}, Abdul Shukor Shamsudin³, Wan Ahmad Fauzi Wan Husain⁴, Mohammad Harith Amlus^{5, 8} and Hariri Hamzah^{6, 8}

¹*School of Human Resource Development & Psychology, Universiti Teknologi Malaysia, Skudai, Johor, Malaysia*

²*Faculty of Business and Management, Universiti Teknologi MARA Cawangan Melaka, 78000 Alor Gajah, Melaka, Malaysia*

³*School of Business Management, Universiti Utara Malaysia, Sintok, Kedah, Malaysia*

⁴*Universiti Malaysia Pahang, Pahang, Malaysia*

⁵*Faculty of Applied and Human Sciences, Universiti Malaysia Perlis, Perlis, Malaysia*

⁶*Universiti Kuala Lumpur (UniKL), Kuala Lumpur, Malaysia*

⁷*ON Semiconductor, Kawasan Perusahaan Senawang, 70450 Senawang, Negeri Sembilan, Malaysia*

⁸*Centre of Excellence for Sport Engineering Research Centre (COESERC), Perlis, Malaysia*

Corresponding author: ^aintanmaizuraar@gmail.com

Abstract. Malaysia is now approaching towards Industrial 4.0. Many initiatives are taken by the government to improve in this digital era. 18.2% contribution towards country's growth domestic product was achieved in 2016 through digital economy which was targeted in 2020 (Malaysia Digital Economy Corporation, 2018). This showed a positive sign that the world is accepting the era of digital technologies in many of the industries including in healthcare. The objective of this research is to determine the factor influencing zero-trust among employees in using technologies in healthcare sector. This research proposed a conceptual framework on Zero trust model for digital employees. The contribution in this research is that it may help Malaysian Productivity Corporation have some information that will be useful to Industry4WRD Readiness Assessment. Furthermore, this research hopes will give insight for Malaysia's National Applied Research and Development Centre (MIMOS) for National Internet of Things Strategic Roadmap.

Keywords: Migration, Industry 4.0, Cyber Security, IoT, Malaysia.

INTRODUCTION

Today's world of business is approaching towards industrial 4.0 where everything was meant to be digitalized. It begins with business transaction, communication and even managing the human resource. In fact, at least 55% of the population around the world have used internet and technologies for day to day basis [1]. Malaysian Government will allocate RM 210 million from 2019 to 2021 to support the transition and migration to Industry 4.0 [2]. Meanwhile, The Malaysia Productivity Corporation (MPC) will carry out Readiness Assessments (Industry4WRD Readiness Assessment) to assist up to 500 Small Medium Enterprises (SMEs) to migrate to Industry 4.0 technologies. Furthermore, with the vision of Malaysia to be regional digital Internet of Things (IoT) development hub, the megatrend has forced the society to implement technology to enhance productivity and to fulfil individual needs.

In addition, managing human resource in organization also has shifted its paradigm from traditional way to modern digitalized method [3]. Now, human resource manager can easily pull a record and statistic about its employees. Similarly, employees in organization can easily access the organization's intranet and improves workplace experience [4]. These two scenarios have raised a concern on security and safety of the data in the company. Despite, the freely usage personal device to access on company's data, record, and files are threatening towards the company. Hence, a basis and fundamental of accessing data should be implemented among digital employees.

In healthcare sector, the glooming of the usage of technology is becoming a norm in the society. Medical doctors, nurses and allied health are adopting technology into their everyday work. Research has proved that medical technology has brought benefit in numerous ways such as a political force to shape social relationships, neutral tools to be interpreted in social interactions and for learning purposes among nurses [5]. Furthermore, Ministry of Health (MoH) has launched Digital Lifestyle Malaysia (DLM): Connected Healthcare to create continuous diagnostics and precision treatment by medical experts utilizing Internet of Things (IoT) technologies ranging from wearable devices that track daily activities, vital signs and diet habits to further merge, dissect and crunch data for biomarkers or measurable indicators. Indeed, the adoption of technology also increased adherence to guideline-based care, enhanced surveillance and monitoring, and helps to decrease medication errors [6].

However, little attention was known in this industry to study the cyber-security in healthcare sector. Evidence shows global average cost of a data breach is \$3.62 million [7]. In healthcare sector, the usage of technology helps to aid the process of management, retrieving medical record history and client's data. This information which easily can be accessed by the medical staff becomes a concern of management. Lack of knowledge and experiences on cyber-attack among medical staff could cause loss for the organization such as losing data, expose of personal data of a client, staff and management's Intel. Hence, to endure this circumstance, zero trust (verify, validate, access) is introduced in the study in order to determine trust (ability, benevolence, integrity) in using the technology.

LITERATURE REVIEW

Zero-Trust

Zero Trust is a security concept grounded in the belief that organizations should not automatically trust anything inside or outside its perimeters and instead must verify anything and everything trying to connect to its systems before granting access [8]. However, ensuring cyber security is a complex task that relies on domain knowledge and requires cognitive abilities to determine possible threats from large amounts of network data [9]. Lack of cognitive ability, awareness, knowledge and experiences can lead to malicious events. This has become a major threat for the organization in the massive implementation of the industrial 4.0 where every employee is expected to be digitalized. However, debates on cyber-attack in the literature and practices were lagging and need more study to explore in the area.

[8] from Forrester Company has developed and believed in the Zero Trust Threat Detection Model. The role of zero trust is important for today's employees, which mean they have to understand every step with precaution when using technology, aware the element of verify when using their own identification, aware in validation a legit data, and accessing information with the right authority to the network. This is pertinent for all digital employees to consider zero trust model in the implementation of their work. In addition, past literature proved that knowledge of cyber security helps in the detection of malicious events [10]. Therefore, this proved that employee personal resource has an impact towards the trust in technology.

Organizational Trust Theory

Gaining employee's awareness in cyber security requires trust. Gaining someone's trust which proposed by organization's trust theory [11] containing three factor which is benevolent, integrity and ability. Instead trust of a person, this research adapted the theory which how people trust in technology. Trust of a person can be affected by employee's personal resource such as experience, awareness, knowledge and relationship. Meanwhile, this research put an added value in this framework by putting the element of zero trust in the relationship between employees' personal resource (experience and awareness) towards the trust in the technology. By adding the zero-trust dimension, which mean an employee whose have experience and awareness in technology will first verify the technology they use, making sure that they are the user (validate) and having the legit access. These zero trusts which means the employee will be more vigilant than they feel they can trust the technology they used.

Besides, responsibility of the digital employees in the workplace is to use, adapt and implemented the technologies in the job. However, without having detail and enough instruction, precaution and awareness of the security, it can be a major cause for an organization to lose its data, through the ignorance and unaware of innocent action of an employee. Hence, the fundamental of being digitalized employee is that, they should be aware and proceed with precaution in accessing and granting the data at the workplace. Therefore, zero trust is important element in determining the relationship between employee experiences and awareness towards trust in technology.

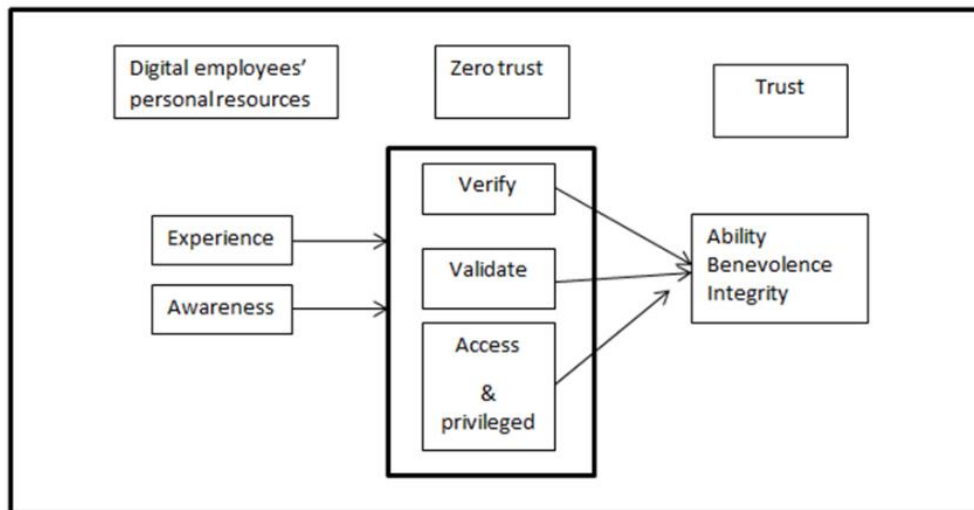


FIGURE 1: Proposed research framework

With proposing framework, therefore the significance of this study will help to support National Transformation Policy (2016-2020) in the New Economic Model to reach high income country through digital transformation. Furthermore, this research hopes will give insight for Malaysia's National Applied Research and Development Centre (MIMOS) for National Internet of Things Strategic Roadmap which envision to create a conducive IoT industry ecosystem which gives impact on employment to create 14 thousand jobs.

Hence, this research gives an output on providing fundamental framework of zero-trust among digital employees which will benefit to the digital literature and realm. The proposed framework in this study also will help Malaysian Productivity Corporation (MPC) in providing data in healthcare sector which hopes will add value in Industry4WRD Readiness Assessment as one of the MPC objectives is to determine the readiness of industry in the adoption of technologies in Industry 4.0.

CONCLUSIONS

The significance of this study will help to support the National Transformation Policy (2016-2020) in the New Economic Model to reach high income country through digital transformation. Furthermore, this research hopes will give insight for Malaysia's National Applied Research and Development Centre (MIMOS) for National Internet of Things Strategic Roadmap, which envision to create a conducive industry ecosystem which gives impact on employment to create 14 thousand jobs.

Furthermore, this research will likely give output on providing a fundamental framework of zero-trust among digital employees, which will benefit to the digital literature and realm. The results in this study also will help the Malaysian Productivity Corporation (MPC) in providing data in the healthcare sector which hopes will add value in Industry4WRD Readiness Assessment, as it is one of the MPC objectives whereby to determine the readiness of the industry in the adoption of technologies in Industry 4.0.

In addition, this study also will help Ministry of Communications and Multimedia Malaysia in supporting the CyberSafe Program where its aim to increases awareness of online safety and security issues among Malaysians while harnessing the benefits of cyberspace.

Meanwhile this research limited to the conceptual framework, and future research should test the relationship and developing instruments for zero trust element instead of adopting and adapting from other scholars.

REFERENCES

1. I. world Stat, "Internet growth statistic (2018)".
2. A. Farrah, "2019 Budget a testament to gov't ambition in accelerating Industry 4.0 adoption," November 2, 2018.
3. D. E. P. and P. S. Strohmeier, "HRM in the digital age – digital changes and challenges of the HR profession," *Empl. Relations*, 2014.
4. K. Dery, I. M. Sebastian, and N. van der Meulen, "The Digital Workplace is Key to Digital Innovation," *MIS Q. Exec.*, 2017.
5. C. Pimmer, P. Brysiewicz, S. Linxen, F. Walters, J. Chipps, and U. Gröhbriel, "Informal mobile learning in nurse education and practice in remote areas-A case study from rural South Africa," *Nurse Educ. Today*, 2014.
6. B. Chaudhry et al., "Systematic review: Impact of health information technology on quality, efficiency, and costs of medical care," *Annals of Internal Medicine*. 2006.
7. N. Mc Carthy, "The Average Cost of A Data Breach Is Highest In The U.S. Data journalist covering technological, societal and media topics.," 2018.
8. J. Kindervag, S. Balaouras, and L. Coit, "Build Security Into Your Network's DNA: The Zero Trust Network Architecture," 2010.
9. N. Ben-Asher and C. Gonzalez, "Effects of cyber security knowledge on attack detection," *Comput. Human Behav.*, 2015.
10. N. Ben-Asher and C. Gonzalez, "Training for the Unknown: The Role of Feedback and Similarity in Detecting Zero-day Attacks," *Procedia Manuf.*, 2015.
11. R. C. Mayer, J. H. Davis, and F. D. Schoorman, "AN INTEGRATIVE MODEL OF ORGANIZATIONAL TRUST.," *Acad. Manag. Rev.*, 1995.
12. Ching, L. L., Ibrahim, S., & Rashid, I. M. A. (2019). An exploration of accountability practices in Non-Governmental Organisation (NGO): Malaysian perspectives. *International Journal of Business and Management*, 1(2), 01-06.
13. Shafiai, S., Rashid, I. M. A., Nasir, N. M., Rahman, S. A., Norman, H., & Ibrahim, S. (2021). Economic determinants tourism performance: Perspective of Thailand's tourism sector. In *AIP Conference Proceedings* (Vol. 2347, No. 1, p. 020279). AIP Publishing.

14. LLC. Husain, W. A. F. W., Ibrahim, S., Yusoff, W. S., Rashid, I. M. A., & Samah, I. H. A. (2021). Introductory analysis of factors affecting intercultural couples in the context of Malaysia. In [AIP Conference Proceedings](#) (Vol. 2347, No. 1, p. 020282). AIP Publishing LLC.
15. Yusoff, Wan Sallha, Intan Maizura Abd Rashid, and Suraiya Ibrahim. "Recent Performance In Singapore's Tourism Industry Using normality Test, Correlation & Regression Analysis: The Effect Of Medical Tourism, Service Sector & Exchange Rate." *European Journal of Molecular & Clinical Medicine* 7.8 (2020): 1354-1362.
16. Samah, Irza Hanie Abu, et al. "The impact of healthcare expenditure and healthcare sector growth on CO2 emission using dynamic panel data system GMM estimation model during COVID 19 crisis." *International Journal of Energy Economics and Policy* 10.6 (2020): 235.
17. Azman, Mohd, et al. "Human Trafficking Policy implementation: the impact of crime rate on instability tourist arrivals in Perlis." (2020).