Journal Homepage: - www.journalijar.com

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH (IJAR)

Article DOI: 10.21474/IJAR01/19294
DOI URL: http://dx.doi.org/10.21474/IJAR01/19294

RESEARCH ARTICLE

FACTORS AFFECTING THE CYBERSECURITY ADOPTION AMONG PLAYERS OF THE MARITIME INDUSTRY, MALAYSIA

Noorsiah Ahmad[1], Nur Aqilah Zainordin[2], Nor Aziyatul Izni[3], Alessia Kum Kah min[1] and Yip Jia Shuen[1]

1. Department of Logistics, Faculty of Business and Management, UCSI University, 56000 Cheras, Kuala Lumpur, Malaysia.
2. Universiti Kuala Lumpur Business School, Malaysia.
3. Centre of Foundation Studies, Universiti Teknologi MARA, Cawangan Selangor, Kampus Dengkil, 43800 Dengkil, Selangor, Malaysia.

Manuscript Info

Manuscript History
Received: 15 June 2024
Final Accepted: 17 July 2024
Published: August 2024

Abstract

Cybersecurity has become a crucial concern in the maritime industry due to numerous cases of notorious cyberattacks that happened in the past which caused major financial losses and the theft of organizations' confidential information. This research investigates the factors encouraging cybersecurity readiness among the players in the maritime industry in Malaysia. Based on 384 responses from maritime and logistics industry in Malaysia using SPSS software to analyse data would identify the organization and environment context can become the factors encouraging the cybersecurity readiness in maritime industry in Malaysia. The finding from the statistical results shows the organizational and environmental context are the factors that affected the cybersecurity readiness in maritime industry in Malaysia.

Introduction:-

Organizations, enterprises, and even governments are benefitted from digital transformation by improving communication transparency, performance effectiveness, and operational cost efficiency (Park et al., 2017). Undoubtedly, this provides a splendid opportunity for businesses or organizations to raise the quality of their products and services by integrating digital technology. Although digital transformation in businesses provides significant advantages, but it also creates chances for information technology safety risks such as cyber-attack on their assets (Rîndașu, 2017). Cyber-attacks can vary from individual attacks to attacks on an organization's confidential data that could destroy the business operation of an organization in any industry including transport, logistics and supply chain. Unauthorized access intrusion into an organization's existing information technology (IT) or information systems (IS) infrastructure can be accomplished through the dispersion of malware, viruses, spyware, and spam on users' emails, which will eventually lead to theft of confidential data (Maurer et al., 2021).

Cybersecurity refers to the application of technologies, processes, and controls that protect confidential data and important systems from cyber threats (Veale and Brown, 2020). It is usually used by any organizations to prevent illegal access to information and other digital systems. A good cybersecurity approach can provide an excellent security infrastructure against malicious assaults designed to gain access, modify, erase, destroy, or ransom sensitive data and systems that belong to the organizations (Kelley, 2022). Cyber security also involves the engagement of people, processes, and technology within the organization to secure the people, operations, and IT infrastructure

Corresponding Author:- Nur Aqilah Zainordin
Address:- Universiti Kuala Lumpur Business School, Malaysia.

collaboratively from cyber-attacks (Ahmed, 2020). Nonetheless, Smith et al. (2010) stated that it involves awareness and strong attachment within organizations to avoid, identify, and defeat cyber-attacks before organizations can possess cyber security. Furthermore, in this research the maritime industry has become more digitalized with technological advancements, it depends on the internet connection for information technology (IT) and operational technology (OT) systems (Kanwal et al., 2022).

Maritime industry development is becoming a major concern because most contemporary ships are well-equipped with computer systems that are used for propulsion, chart creation, navigation, and other functions (Bielawski and Lazarowska, 2021). Maritime operations play important roles to fulfil supply and demand in international business. Undoubtedly, cybersecurity has become a crucial topic in the maritime industry due to numerous reported cyberattacks that resulted in significant financial loss, as well as the violation of organizations' sensitive information. Thus, the objective of cyber security is of the utmost importance currently, especially in the maritime industry. The safety of the crew and cargo on board, the ship's function, may be severely jeopardized by OT system malfunctions. Similarly, dangerous circumstances could arise from the failure of specific IT systems, such as the inability to promptly obtain a manifest of dangerous products (Veale and Brown, 2020). The purpose of this study was to study how organizational context and environmental context affect cybersecurity adoption and practiced with knowledge and skill among the players in the maritime industry in Malaysia.

Literature Review:-

Theory of Acceptance (TAM)

Theory Acceptance Model (TAM) used in this study and supported on the Cybersecurity applied in maritime industry. According to Addae et al. (2019), the Technology Acceptance Model (TAM) variables including perceived usefulness and perceived ease of use have significant impacts on the usage of cybersecurity. The TAM framework created by Davis (1989), is one of the most significant research models in studying the acceptance of information systems and information technology. This is evidenced by numerous research that demonstrated TAM has been successfully applied in the context of online learning (Giesbers et al., 2013; Shin and Kang, 2015; Tarhini et al., 2016).

Technology Acceptance Model (TAM) is also a three-stage process wherein external forces set off cognitive reactions (perceived ease of use and perceived usefulness), which in turn create a perceptual response (attitude toward using technology), impacting use behavior (Davis, 1989; Davis, 1993). TAM depicts behaviour of maritime organizations as the result of perceived usefulness, perceived ease of use, and behavioral intention as shown in Figure. Expectations of successful behavioral outcomes and the conviction that behavior does not need much effort are conveyed by perceived ease of use and perceived usefulness (Davis, 1989). This theory will used on the perspectives of application on cybersecurity by the maritime organizations in perspective the top management support, organization skill and culture.

Cybersecurity Adoption

Cybersecurity adoption is the capability to adopt and apply to network intrusions, malware attacks, phishing scams, and theft of data and intellectual property from both inside and outside the network (Sullivan, 2016). Moreover, cybersecurity framework can measure cybersecurity adoption with the result to improve the infrastructure of cybersecurity (Eilts, 2020). NIST Cybersecurity Framework is the latest version to evaluate and practice cybersecurity that consists of several high-level functions (Chapman & Reithel, 2021). There are five functions of the framework including "identity, protect, detect, respond and recover." Besides, cybersecurity in the logistics system including maritime operations is essential for ensuring a secure and dependable flow of goods and services. It is vital part of risk management for companies, guarding them against any security lapses and guaranteeing the continuity of their operations (Al-Bkree, 2023; Enache, 2023).

Simply, Ten et al. (2010) state that "identify" is performing vulnerability analyses, and monitoring computer ports for signs of cyberattacks, which is the activity to comprehend the risks associated with cyber security. Besides, recovery is the process of developing and making necessary actions to uphold resilience plans and restore any capabilities or services that were damaged as a result of a cybersecurity incident (Chapman and Reithel, 2021). In order to mitigate the effects of a cybersecurity incident, recovery needs to timely restore normal operation (Eilts, 2020). Moreover, information security can be demarcated in terms of technical, formal, and informal levels. On a technical level stated that information security controls in computer systems include speech analysis, firewalls, digital signatures, and other methods to protect software, devices, and data within the computer system (Khan et al.,

2022; Alshurideh et al., 2023). All these methods are used to protect the applications of software, devices, and data that are within the computer system itself. Besides, at the formal level, official controls are established based on rules that state how the published technical controls should be structured.

Organisational Context

Organizational context refers to the organizational functionalities and characteristics that will influence the decision to adopt an advancement (Cantisani, 2006). According to Hsu et al., (2012), organizational factors described in earlier studies involve top management support, organizational skills, as well as organizational culture. This study is focusing the maritime organization that influence the adoption and practice of cybersecurity in technology advancement.

Top Management of Maritime Organization. According to Daud et al. (2018), cybersecurity practice is impacted by top management support in the maritime organization. This means that support from top management is essential and crucial to an organization's cybersecurity implementation (Sumner, 2009). For instance, Kwon et al. (2012) suggested that top management may influence employees' behaviors toward the organization's security protocols and policies. However, such an influence requires top management engagement and commitment. As a result, a key aspect to be examined is the dedication of top management toward cyber security (Daud et al., 2018).

In the maritime sector, top management needs to take note that policies and procedures must be developed according to the International Maritime Organization (IMO) criteria, considering the pertinent standards and rules, to ensure the safety of ships, crew, and the preservation of the marine environment (Kanwal et al., 2022). The serious involvement of top management of the organization to ensure the any policies and procedures set will be successful implemented and achieved the goals of the organization.

Maritime Organizational Skills and Culture on Cybersecurity Adoption. Recent cyber incidents in the marine sector have shown that many employees lack the necessary training to respond to cyber threats, which may cause them to behave in ways that are reluctant to help reduce risks and manage the problem. To have efficient maritime cyber management, the IMO claimed that there is an imperative need to increase awareness of information security systems (Kanwal et al., 2022). Hsu et al. (2012) also claimed that the collaborative culture of an organization can greatly affects an organization's performance by motivating team members to contribute and raise their sense of accountability for the organization's cyber security. Moreover, organizational context is essential for encouraging cybersecurity adoption as evidenced by previous studies discussed above.

Environmental Context

Environmental context is the external environment of an organization that forces the industry to use emerging technology to operate a business in society (Nasrudin, 2022). The general environment will provide impact indirectly a company with the demographic, technological, sociocultural, and political-legal sectors (Butt, 2013). The description of these general environment as below:

Demographic and Sociocultural.

Within such an emerging environment, a critical requirement towards safe and secure information society is to prepare people, aligned with contemporary societal needs, to encounter future challenges in their personal and professional life. The main challenges are related to our increasing dependency on digital technologies and the corresponding needs to improve cybersecurity awareness (Gunleifsen et al., 2019). The maritime industry should be aware of cyber attacked and apply the practice of safe and secure emerging trends of the industry on information technology in their day-to-day practice. The knowledge and skills by the society able to protect them from the cyber-attack on the information technology.

Technological.

The discussion above has clearly stated previous studies about the positive relationship between the independent variable and the dependent variable. It also matches with the Technology Acceptance Model (TAM) due to the players are encouraged by environmental contexts to use cybersecurity (Hasan, 2021).

Political

Legal. Political-legal is related to government including government regulation and government support that can result in a successful business by conducting cybersecurity in the maritime industry. Secondly, the environmental

context in an indirect environment is government regulation. Regulation is the law set by the government which is the parties have the authority and power to control players' behavior to operate a business in the industry (Ruggie, 2018).

Malaysia does not have a standalone cybersecurity law, but there is a patchwork of laws to combat cybercrime in 2018. For example, the existing cybersecurity legislations are the Computer Crimes Act 1997, the Communications and Multimedia Act 1998, the Copyright Act 1987, Personal Data Protection Act 2021, Digital Signature Act 1997, Strategic Trade Act 2010, and Sedition Act 1948 (Yik, 2018).The researcher also concluded the ability of the government to form cybersecurity law can result in the need for cybersecurity readiness in an indirect environment of the industry (Wall et al., 2015).

Conceptual framework

Figure 1 shows the conceptual framework for this study.

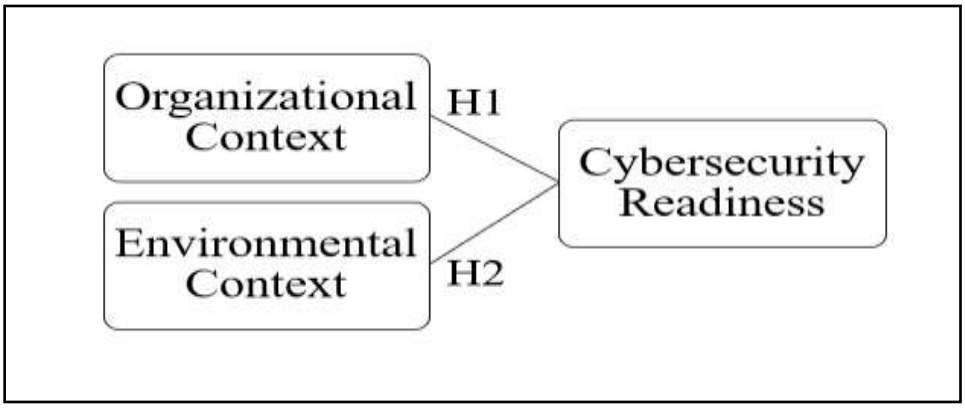

Figure 1:- Conceptual framework (original).

Methodology:-

Data Collection

This study employed a quantitative method to test the sample of respondents. The research used non-probability to analyse the data. In addition, the study adopted convenience sampling to distribute the online questionnaire via Google Forms, WhatsApp, Facebook, and Telegram to the respondents. The sample for this research was respondents who lived in Klang Valley as the target is that there are many companies that offer shipping and logistics services. The sample size of the respondents was 384, based on Krejcie and Morgan (2016). The questionnaire was divided into three sections: sections A, B, and C. The questionnaire was adopted from the previous study. The questionnaire was designed using a five-Likert scale. The study was using SPSS to test the relationship between the organization and environment context (independent variables) and the cybersecurity adoption among the players of maritime industry (dependent variable).

The study used SPSS software to analyse the hypotheses from the study. The study will test their reliability using Cronbach's alpha. Another analysis that will be tested is multiple linear regression to test the relationship between the independent variables and the dependent variable. Lastly, the study will assess Spearman's correlation coefficient to measure and direct the relationship between two or more variables (Obilor and Amadi, 2018). It is suitable to apply when both variables represent the ordinal scale of measurement such as Likert Scale (Samah, 2018).

Results and Discussion:-

Descriptive Analysis

Based on the results, after distributed 400 questionnaires there were 384 respondents who answered the distributed questionnaire. From the results, 172 (44.8%) respondents were male, and 212 (55.2%) respondents were female. From the results, most of the respondents 64.6% are from non-managerial staff, 12.8% from middle managers, and 15.9% from first line manager. Most of the respondents are coming from various aspect of the industry that utilizing the logistics services, 384 respondents, there are 168 respondents working in the maritime industry, 30 people from

the land transport industry, 92 people from the freight forwarding industry, 30 people from the airline industry, and 64 people from another side of the industry.

Spearman's Correlation Coefficient Analysis

There is a correlation as the independent variables (Organizational Context and Environmental Context) and dependent variable (Cybersecurity Adoption) has a significant positive relationship with 2-tailed at the 0.01 level. Table 2 shows Organizational Context has a positive and very strong relationship with the dependent variable, Cybersecurity Readiness ($p = 0.816$, $0.80 \leq p \leq 1.00$). Besides, Environmental Context also has a positive and strong relationship with the dependent variable, Cybersecurity Readiness ($p = 0.776$, $0.60 \leq p \leq 0.79$). Hence, it indicates that organizations in the logistics field generally and maritime industry specifically are aware of cybersecurity and adopt cybersecurity in the workplace along the maritime operations.

Table 1:- Spearman's Rho test on the relationship between independent variables and dependent variable.

		Organizational Context	**Environmental Context**	**Cybersecurity Readiness**
Spearman's Rho	Organizational Context	1.000		
	Environmental Context	.751**	1.000	
	Cybersecurity Readiness	.816**	.776**	1.000

Table 2:- Summary of Spearman's Rho test for each independent variable with dependent variable.

Independent Variables	**Spearman's Correlation Value, p**	**Strength of Association**
Organizational Context	.816**	Very Strong
Environmental Context	.776**	Strong

Multiple Regression Analysis

Based on Table 3, there is value R and R Square. The value can be used to indicate the proportion of the total variation between the dependent variable (Cybersecurity Adoption) and independent variables (Organizational Context and Environmental Context). The result of multiple regression analysis in this research is 0.832 and 0.831 for adjusted R Square. It shows that there is a total variance of 83.2% in the dependent variable and 83.1% in the independent variable.

Table 3:- R square value.

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.912[a]	.832	.831	.32795
[a] Predictors: (Constant), Environment Context, Organizational Context				

Discussion on the Finding:-

The logistics industry and other relevant industry have responded to the study on the factors affecting to the cybersecurity adoption among the players among the maritime industry. The factors identified were the organization context and environment context supported the positive impact on the cybersecurity adoption in the industry. The discussion on the finding as below:

Organization Context:

The result from analysis of Spearman's Correlation Coefficient Test, the ρ-value of Organizational Context is 0.816 for the first hypothesis. It shows that there is a very strong and positive relationship between the independent variable (IV), Organizational Context, and the dependent variable (DV), Cybersecurity Adoption. This is since the ρ-value of 0.816 lies between 0.80 and 1.00 which indicates the strongest correlation degree based on Spearman's Rank-Order correlation. Therefore, there is a significant relationship between Organizational Context and Cybersecurity Adoption by the organization in Maritime industry. The discussion of the result that the organizational context consists of maritime organization's top management support, organizational skill and organizational culture connected strongly in cybersecurity adoption. The maritime industry is adopting and applying the cybersecurity system in the maritime operations to protect their information technology against any cyberattacks.

The participation and strong involvement of top management in cybersecurity adoption in the organization is very important. The top management created the teams to explored on the issues of cyber-attacked on their information technology of the business. They will decide and adopt the cybersecurity system after having the research on the current situation and possible future cyber threat. The right selection and adoption of cybersecurity system, they also need to ensure the organization aware on the issues and proper training on the selection cybersecurity will be managed systematically. The cybersecurity adoption with skills and become organizational culture for the organization. Beside that the collaboration among the players on the cybersecurity can be adopted by others in the maritime industry for the sustainability of the business.

The continuous awareness and training in adopting and practicing the cybersecurity system among the organization members and the organizational culture created to ensure on their information's privacy protection from the cyberattack of the digital application of the organization. The skills on their digital application on maritime operations with the skills on cybersecurity system will strengthen themselves from the cyber threats. The organizational skills and organizational culture on the cybersecurity adoption can be implemented successfully.

Environmental Context.

The finding on the same Spearman's Correlation Coefficient Test, the ρ-value of Environmental Context is 0.776 for the second hypothesis. It shows that there is a strong and positive relationship between the independent variable (IV), environmental context, and the dependent variable (DV), Cybersecurity Adoption. This is since the ρ-value of 0.776 lies between 0.60 and 0.79 which indicates the second strongest correlation degree in Spearman's Rank-Order correlation. This indicates that most organizations get to solve issues more rapidly as they exploit knowledge learned from their competitors past experiences. The maritime organizations also adopting the information related to political-regulation policies, demographic and sociocultural will assist them on the application on the cybersecurity system designed and practiced. Organizations in maritime industry that are constantly updated on new attacks by their competitors are more prepared to defend against cyber-attacks, highlighting the critical role of information exchange between competitors in increasing cybersecurity adoption and practicing.

In this study, it was proposed that Environmental Contexts that influence an organization's adoption to safeguard its cyber infrastructure and services include collaboration with a society, competitor, government regulation, and government support. This finding is consistent with previous studies' findings which emphasized organizations that collaborate with their competitors are more ready to defend against cyber-attacks (Nagurney & Shukla, 2017; Casino et al., 2019). The result and analysis have proving that the information technology adopting and applying by the global maritime industry aware on the cyber threat and taking the serious effort on the cybersecurity to protect themselves on the attacked of their information privacy and any related matters to ensure of their sustainability in the marketplace. The efforts on improving the cybersecurity adoption on the maritime operations must be continuously monitor and based on the emerging trends from the global market. Adopting and applying the digital application in business perspective is important and should be aligned with the protection on the system for any organization in the world.

Conclusion:-

In conclusion, the independent variables namely Organizational Context and Environmental Context have a direct as well as significant impact on the dependent variable, which is the adoption of cybersecurity among the players in the maritime industry. Given that Organizational Context had the largest unstandardized beta value (0.601) in the Multiple Linear Regression analysis, thus it has been identified as the most significant of these two IVs. Similar to the earlier analysis on Spearman's Correlation Coefficient Test, it shows that the respondents perceived top management support, organizational skills, and organizational culture to play an important role in encouraging cybersecurity adoption in the organization. Such perceptions of the respondents have a positive attitude toward cybersecurity selection as they consider the protection of the asset and data will be significantly enhanced with the strong implementation of organizational context.

The findings of this study can help the government, banks, and all relevant companies in the logistics and maritime industry sector, as the study has filled in the gap that previous research lacked, whereby most research studies focused on examining the cybersecurity adoption among players in the maritime industry in Malaysia. Besides that, this study would help future studies can used the factors of the application of cybersecurity system among the market players in the maritime industry, as this study support further research on the improvement of cybersecurity

system that already adopted for future preparation. This can either go beyond or delve deeper into the two variables, as well as other variables.

References:-

1. Alshurideh, M., Alquqa, E., Alzoubi, H., Kurdi, B., & Hamadneh, S. (2023), "The effect of information security on e-supply chain in the UAE logistics and distribution industry", Uncertain Supply Chain Management, Vol. 11, No. 1, pp. 145-152.
2. Al-Bkree, M. (2023), "Managing the cyber-physical security for unmanned aerial vehicles used in perimeter surveillance", International Journal of Innovative Research and Scientific Studies, Vol 6, No. 1, pp. 164-173.
3. Ahmed, E. M. (2020), "Modelling information and communications technology cyber security externalities spillover effects on sustainable economic growth", Journal of the Knowledge Economy, pp. 10–11. https://doi.org/10.1007/s13132-020-00627-3
4. Addae, J. H., Sun, X., Towey, D., and Radenkovic, M. (2019), "Exploring user behavioral data for adaptive cybersecurity", User Modeling and User-Adapted Interaction, Vol. 29, No. 3, pp. 701–750. https://doi.org/10.1007/s11257-019-09236-5
5. Butt, S. (2023), "Specific or general environment", available at: https://www.slideshare.net/saqibazhar/specific-or-general-environment (accessed 01 November 2023)
6. Bielawski, A. and Lazarowska, A. (2021), "Discussing cybersecurity in maritime transportation", Maritime Technology and Research, Vol. 4, No. 1, 20–22. https://doi.org/10.33175/mtr.2022.252151
7. Cantisani, A. (2006), "Technological innovation processes revisited", Technovation, Vol. 26, No. 11, pp. 1294–1301. https://doi.org/10.1016/j.technovation.2005.10.003
8. Chapman, T. A. and Reithel, B. J. (2021), "Perceptions of cybersecurity readiness among workgroup IT managers", Journal of Computer Information Systems, Vol. 61, No. 5, pp. 438-449. https://doi.org/10.1080/08874417.2019.1703224
9. Daud, M., Rasiah, R., George, M., Asirvatham, D., and Thangiah, G. (2018), "Bridging the gap between organisational practices and cyber security compliance: Can cooperation promote compliance in organisations?", International Journal of Business & Society, Vol. 19, No. 1, pp. 161-180.
10. Davis, F. D. (1989), "Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology," MIS Quarterly, Vol.13, No. 3, p. 319. https://doi.org/10.2307/249008
11. Enache, G. I. (2023), "Logistics Security in the Era of Big Data, Cloud Computing and IoT," Proceedings of the International Conference on Business Excellence, Vol. 17, No. 1, pp. 188-199.
12. Giesbers, B., Rienties, B., Tempelaar, D., and Gijselaers, W. (2013), "Investigating the relations between motivation, tool use, participation, and performance in an e-learning course using web-videoconferencing", Computers in Human Behavior, Vol.29, No.1, pp. 285–292. https://doi.org/10.1016/j.chb.2012.09.005
13. Park, Y., El Sawy, O. A., and Fiss, P. C. (2017), "The Role of Business Intelligence and Communication Technologies in Organizational Agility: A Configurational Approach", Journal of the Association for Information Systems, 18(9), pp. 648–686. https://doi.org/10.17705/1jais.00467
14. Rîndașu, S.-M. (2017). Emerging information technologies in accounting and related security risks – what is the impact on the Romanian accounting profession. Journal of Accounting and Management Information Systems, Vol. 16, No. 4, pp. 581–609. https://doi.org/10.24818/jamis.2017.0400
15. Maurer, C., Kim, K., Kim, D., and Kappelman, L. A. (2021), "Cybersecurity. Communications of the ACM", Vol. 64, No. 2, pp. 28–30. https://doi.org/10.1145/3399667
16. Veale, M., and Brown, I. (2020), "Cybersecurity", Internet Policy Review, Vol. 9, No. 4, pp. 20–22. https://doi.org/10.14763/2020.4.1533
17. Nasrudin, A. (2022), "Technological Environment: Definition and Its Effect on Business", available at: https://penpoin.com/technological-environment/ (accessed 01 November 2023)
18. Kelley, K. (2022), "What is Cybersecurity and Why It is Important?" available at: https://www.simplilearn.com/tutorials/cyber-security-tutorial/what-is-cyber-security (accessed 01 November 2023)
19. Smith, Winchester, Bunker, and Jamieson. (2010), "Circuits of power: A study of mandated compliance to an information systems security "de jure" standard in a government organization", MIS Quarterly, Vol. 34, No. 3, p. 463. https://doi.org/10.2307/25750687
20. Shin, W. S., and Kang, M. (2015), "The use of a mobile learning management system at an online university and its effect on learning satisfaction and achievement", The International Review of Research in Open and Distributed Learning, Vol.16, No.3. pp. 110-130. https://doi.org/10.19173/irrodl.v16i3.1984

21. Sumner, M. (2009), "Information security threats: a comparative analysis of impact, probability, and preparedness", Information Systems Management, Vol. 26, No.1, pp. 2-12. https://doi.org/10.1080/10580530802384639
22. Tarhini, A., Elyas, T., Akour, M. A., and Al-Salti, Z. (2016), "Technology, demographic characteristics, and E-learning acceptance: A conceptual model based on extended technology acceptance model", Higher Education Studies, Vol. 6, No. 3, p. 72. https://doi.org/10.5539/hes.v6n3p7
23. Ten, C. W., Manimaran, G., and Liu, C. C. (2010), "Cybersecurity for critical infrastructures: Attack and defense modelling", IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans, Vol. 40, No. 4, pp. 853-865. http://dx.doi.org/10.1109/TSMCA.2010.2048028
24. Kanwal, K., Shi, W., Kontovas, C., Yang, Z., and Chang, C.-H. (2022), "Maritime cybersecurity: are onboard systems ready?", Maritime Policy & Management, pp.1-19. https://doi.org/10.1080/03088839.2022.2124464
25. Khan, A. A., and Abonyi, J. (2022), "Information sharing in supply chains-Interoperability in an era of circular economy", Cleaner Logistics and Supply Chain, p. 100074.
26. Kwon, J., Ulmer, J. R., and Wang, T. (2012), "The Association between Top Management Involvement and Compensation and Information Security Breaches", Journal of Information Systems, Vol.27, No.1, pp. 219–236. https://doi.org/10.2308/isys-50339
27. Ruggie, J. G. (2018), "Multinationals as global institution: Power, authority and relative autonomy", Regulation & Governance, Vol.12, No.3, pp. 317-333. https://doi.org/10.1111/rego.12154
28. Yik, C. S. (2018), "Basics of Cyber Security Law in Malaysia", available at:https://chialee.com.my/basics-of-cyber-security-law-in-malaysia/ (accessed 01 November 2023)
29. Wall, J., Lowry, P. B., and Barlow, J. B. (2015), "Organizational violations of externally governed privacy and security rules: Explaining and predicting selective violations under conditions of strain and excess", Journal of the Association for Information Systems, Vol. 17, No.1, pp. 39-76. https://doi.org/10.17705/1jais.00420.