Role of Mode of Business on Level of awareness of cyber crime

The Journal of Educational Paradigms
2023, Vol. 02(02) 206-211

ISSN (Print): 2709-202X
ISSN (Online): 2709-2038
DOI:10.47609/0202022023

Logeswaran Ramayah[1], Saralah Devi Mariamdaran Chethiyar[2], Yadu K Damodaran[3]

Abstract

Cybercrime remains a challenge for businesses across the world. In recent years business has been spending a huge budget on cybercrime protection mechanisms. However, awareness of cybercrime is considered the initial point before planning investment in cybercrime protection mechanism. The purpose of the study was to evaluate the association between nature of business and cyber-crimes in Malaysia. To achieve the research objectives of the current study data has been collected from the entrepreneurs working in the state of Penang using the purposive sampling technique. A sample of 350 respondents has been taken for the data analysis. The results indicate the nature of business correlated with cybercrime awareness. The empirical findings of PLS-SEM revealed that cyber-crimes are increasing because of the type of business which is more prone to the risks associated with the nature of the business. The findings of the current study outline the implications for policymakers, regulatory authorities, and entrepreneurs.

Keywords: Business mode, Position, cyber-crimes, and awareness.

The Malaysian business community is currently facing the threat of cyber-attacks especially in recent years. According to a report released by the Malaysian government, there were more than 11,875 cybercrime cases reported after the year of 2019 in which most of it involved Small and Medium-sized Enterprise (SME). Furthermore, after the implementation of the Movement Control Order (MCO), more than 78% of SMEs have directed their focus towards online platforms to reduce investment in business infrastructure thus making them more susceptible to cyber security issues (kkmm.gov.my, 2022). Hence, the "National Cyber Security Agency" (NACSA) is attempting to offer potential solutions, therefore have closely observed the serious attention paid to current "cyber security" issues. In addition, the "National Cyber Crisis Management Plan" has been initiated by the Malaysian government to reduce the number of a of attacks on businesses.

Cybercrime is harmful software developed by online criminals with the express purpose of damaging computer, network, and ICT infrastructure and generating revenue. Businesses without adequate cybersecurity protection plans or inadequate funding for cyber defense efforts, including increasing human capacity and competence, won't Cybercrime be harmful software developed by online criminals with the express purpose of damaging computer, network, and ICT infrastructure and generating revenue. Businesses without adequate cybersecurity protection plans or inadequate funding for cyber defiance efforts, including increasing human capacity and competence, won't survive a cyber event. SME Association of Malaysia noted that cyberattacks are growing increasingly and are widespread among firms. Nonetheless, given their limited resources and ignorance of cyberthreats, it is concerning that the majority of SMEs are still not adequately prepared to protect their digital systems (The Star, 2021). Eeten and Bauer (2008) also highlighted that an infected end user's system, particularly one that belongs to a small business, is readily penetrated owing to a lack of cybersecurity understanding and cyber protections.

In recent years, cybercrime rates have increased in Malaysia, affecting individuals, large and small businesses, and institutions alike (Monteith, et. al., 2021). Hackers steal crucial business-related information, resulting in frequent losses for businesses, which require significant financial investment to recover. According to (Tharshini, Hassan, & Mas'ud, 2021). cyber security-related threats are emerging as a result of Malaysia's growing internet penetration. However, the majority of businesses are dealing with "cybercrime" issues as a result of using third-party websites and making online payments to their customers. Companies are currently attempting to reduce the use of third-party applications in order to reduce the likelihood of cyber-attacks against their technological systems.

Additionally, according to a statistic provided by the Malaysian Computer Emergency Response Team (MyCERT), there were about 8,366 occurrences of cybercrime recorded in Malaysia between January 2020 and September 2020. (The Star, 2021). In addition, cybercrime incidents have increased significantly in Malaysia during the enforced MCO, as evidenced by the 3,906 complaints made to the Cyber999 Help Center between 18 March 2020 and 30 June 2020 regarding cyberbullying, hacking attempts,

[1] Master's Student of Science (Correctional Science), Psychology & Counselling Program, School of Applied Psychology, Social Work and Policy, College of Arts and Sciences, University Utara, Malaysia, Malaysia, Corresponding author: logeswaranpdrm@gmail.com
[2] University Lecturer Psychology & Counselling Program, School of Applied Psychology, Social Work and Policy, College of Arts and Sciences, University Utara, Malaysia, Malaysia, Corresponding author: devi@uum.edu.my
[3] Master's Student of Social Work (Clinical and Community Practice), School of Sociology and Social Work, Christ Deemed to be University, Bengaluru, Karnataka, India. Corresponding author: yadudk023@gmail.com

cyber intrusions, and cyber-fraud in urban areas with a high-speed internet connection (The Star, 2020). Also, a total of 4,615 cybersecurity events were reported to Cyber Security Malaysia between January 2021 and May 2021, including examples of online fraud (3,299 cases), infiltration (765 cases), and the dissemination of dangerous code to the computer and/or mobile phone (256 cases) (The Star, 2021).

The most recent occurrence of an Advanced Persistent Attack (APT) against Malaysia used email spear phishing as its method of manifestation. According to the national cyber security, from 2016 to 2018, there was an increase in the rate of cybercrime as shown in table 1.2. Given that many Malaysian firms continue to use a lot of outdated and unsupported systems that cannot be updated with the most recent security updates, these dangers might become more serious. Many flaws in these outdated systems might make them vulnerable to attacks and the tools used by cybercriminals.

Hence, one of the contributing factors to the cybercrime incidence is the lack of cybersecurity awareness as mentioned by Communication and Multimedia Minister, Datuk Zahidi Zainal Abidin (The Star, 2021). Therefore, the National Cyber Security Awareness Module and Cyber Security Enhancement Initiative for SMEs have been established by the Ministry of Communications and Multimedia (MCMC) to inform the public about cyberthreats and how they may defend themselves. Besides, there is also a drawback in the legal system throughout the world that has a difficult time controlling the Internet (Jiow, 2013). As a result, cybercrimes pose fresh difficulties for policymakers, law enforcement officials, and international organizations.

It has been claimed that because Malaysia does not currently have a data protection policy to protect internet users' personal information, cybercrime incidents are more likely to occur. According to (Ibrahim et al., 2021), one of the factors contributing to the recent increase in attacks is inadequate government-affiliated organization monitoring of "cybercrime" control. For instance, in 2014, three well-known Malaysian banks—Affin Bank, Al-Rajhi Bank, and Bank of Islam—incurred a loss of RM 3 million. It has revealed that 5956 "telecommunication Frauds" occurred primarily in Malaysia and that approximately 3200 "e-commerce"-related frauds occurred between 2018 and 2019 (kkmm.gov.my, 2022).

The ongoing problem for an administrative body is cybercrime. The discussion of this study has also assisted in evaluating the Malaysian government's recent initiatives to lower the incidence of "cybercrimes." The results of the investigation could therefore be advantageous to combat cybercrime activities especially. Additionally, this investigation will look at how the controlling structure is used and what that means for the company.

Literature Review

According to Duryana Mohamed (2012), to effectively investigate cybercrimes, one must be totally committed and prepared to take on criminals. This means that in addition to being ready to deal with the repercussions, the investigating officer or other authorized person must also possess the information and abilities necessary to identify the suspect and look into cybercrime situations. It is essential to have enough statutory provisions and efficient procedural laws in place in order to handle the challenges that lie ahead. In order to maintain the efficiency of the investigative process, it is crucial to adhere to the established procedures and best practices. The purpose of this study is to investigate the procedures for conducting cybercrime investigations in accordance with the 17 Criminal Procedure Code (CPC) and Malaysian cyberlaws in order to pinpoint any shortcomings and difficulties discovered by investigators. The Criminal Process Act, the Communications and Multimedia Act, and the Computer Crimes Act of 1997 would be the primary sources of information. The background information will also make mention of other legislation.

This research examines moral behavior, usage, and compliance with computer or internet security, which is connected to the Theory of Planned Behavior. (Ifinedo, 2012). Although the application of preventive measures is not directly impacted by self-control, intention is. Subject norms, which are crucial for line protection, are weak. Self-efficacy and online experience have an impact on self-control.

An organization must exercise self-control to prevent becoming a victim of cybercrime and be aware of online hazards. Cybercrime can be decreased if employees are more committed to raising awareness and information about it. According to research by Furnell, Gennatou, and Dowland from 2002, people are unsure about what to do to increase their cyber security. Cybercriminals may target them if they are not aware. In order to address the issue of cybercrime, it is crucial to be aware of it.

Furthermore, theory of reasoned action should be addressed. The two categories of knowledge are procedural and declarative (Page & Uncles, 2004). Declarative knowledge is an actual condition that has an online explanation. For instance, a slow internet connection. Use of the internet generally is also stated to be part of declarative knowledge (Potosky, 2007). Moreover, procedural knowledge includes dynamic data about policy activities (Page & Uncles, 2004). Thus, having knowledge is crucial when utilizing a computer or the internet. To prevent cybercrime, internet literacy is equally crucial.

According to Malaysia Digital Corp (MDEC), which projected a loss of RM 51 billion due to cyber security threats in Malaysia, accounting for more than 4% of the country's total gross domestic product, cybersecurity helps to reduce cyberthreats that could threaten the country's sovereignty and economy. (Business Today, 2021). According to local police reports in Business Today news in 2021, there were 4,327 cybercrime incidents recorded in the first quarter of this year, resulting in losses of RM77 million, down from 14,229 cases reported in the same period last year, which resulted in losses of RM413 million.

Cybercriminals employ malware to disable and even injure host systems in order to steal money. Cybercrime is a sort of crime that occurs online. They partially hack and partially expose private photographs, data, and other information. In this day and age, the structure of Malaysia's rules and regulations is quite successful against cybercrime. On the other hand, it is also evident that commercial groups are concerned about the situation in this nation (Abdullah et al., 2018). The Malaysian corporate workforce may be significantly impacted by this method. On the other hand,

(Abiodun & Abioro 2020.) assert that the people of this country are utterly terrified of the unlawful activities carried out by cutting-edge software and technology. Because of this, the government of this country must now safeguard the security and privacy of its inhabitants.

Research Methodology

In this study, the researcher has chosen a quantitative research type of study survey. The location of this study was Gelugor, Penang. Gelugor is a location in the Malaysian state of Penang. Gelugor, Penang was a convenient location for the researcher to conduct his or her investigation because it is close to a number of small and medium-sized businesses. The researcher can also carry out a data collection procedure without encountering any difficulties. As one of the ethical and legal requirements in research involving human participants, consent forms issued to all parties engaged in this experiment prior to the research's start. In total 350 participants were chosen as samples for the current study using purposive sampling technique based on the morgan table. The questionnaire provided to the study participants after everyone agrees. The data has been collected using the pre-developed instruments from prior studies.

Analysis

After conducting the preliminary tests and ensuring that the instrument is reliable, inferential statistics have been conducted. The result of the regression analysis revealed the following confirmation of the hypothesis testing.

Table 1: Reliability Analysis

	Cronbach's Alpha	Composite Reliability	Average Variance Extracted (AVE)
Mode of Business	0.942	0.904	0.733
Level of awareness of cyber crime	0.956	0.996	0.714

After ensuring that the instrument is reliable and valid, the hypothesis testing has been made.

Table 2: Regression Analysis

	Coeff.	**S. D**	**T-Values**	**P Values**
Mode of Business -> Level of awareness of cyber crime	0.245	0.113	2.169	0.031

Conclusions

This study aims to identify the level of awareness of cybercrime among entrepreneurs in recent times. Because the Malaysian government took the initiative to introduce the Malaysia Cyber Security Strategy (MCSS) 2020–2024 to improve cybersecurity preparedness and for building a strong infrastructure for antimalware solutions, and cybersecurity Malaysia, this can be said to be a national occurrence. As a result, the national cybersecurity authorities also published a study revealing that on average, 31 incidents of cybercrime are reported in Malaysia each day.

The implication of this study is that the researcher can get a clearer view of the level of cybercrime awareness among entrepreneurs and facilitate future research in similar perspective. In addition, the researcher also learned more about differences in the level of cybercrime based on the position in organization and mode of business. The Malaysian ministry of education will be able to determine the degree of cybercrime knowledge among businesses from this survey and will be able to act to raise that awareness. However, the Ministry of Communications and Multimedia will be able to use this knowledge to improve cybersecurity going forward to avoid cybercrime.

The researcher made several recommendations that will make future investigations easier. One of the recommendations for improvement is that future researchers widen the scope of their research by concentrating on enterprises and including all of Malaysia's entrepreneurs. In addition to their degree of education, the researcher may also examine the reasons why business owners have a moderate level of awareness of cybercrime and the reasons why there are changes in those levels depending on the position of the business owners within the company. Next, business owners can increase the number of responders to obtain more accurate results. The researcher made several recommendations that will make future investigations easier. One of the recommendations for improvement is that future researchers widen the scope of their research by concentrating on enterprises and including all of Malaysia's entrepreneurs. In addition to their degree of education, the researcher may also examine the reasons why business owners have a moderate level of awareness of cybercrime and the reasons why there are changes in those levels depending on the position of the business owners within the company. Next, business owners can increase the number of responders to obtain more accurate results.

The results of this study can also be used by researchers to develop educational modules that would make entrepreneurs more aware of cybercrime. This session can assist business owners in learning how to spread the word about cybercrime. Future research can instead concentrate on qualitative study as this study covers quantitative investigation, which makes use of questionnaires to collect more information in greater depth. h. Because respondents must be questioned in-person, prejudice present in questionnaires may be eliminated in qualitative research, which is also more accurate and honest.

The sampling of this study only covers entrepreneurs who is running a small medium based Enterprise (SME) businesses in Gelugor, Penang. Therefore, it cannot be generalized to entrepreneurs in other places and the data cannot be considered as a generalized data nationwide.

In order to collect data for this study, a questionnaire was provided to respondents who are business owners in Gelugor, Penang. In this study, the researcher also used the stratified sampling technique. 250 business owners in Gelugor were chosen at random by the researcher to participate in this survey as responders. The study's findings indicate that entrepreneurs have a modest level of knowledge about cybercrime. As a result, this study can inform business owners about cybercrime and increase awareness of it among local business owners. According to this study, they may also observe how the level of knowledge of entrepreneurs about cybercrime varies depending on their line of work and position within an organization according to this study.

References

Abbasi, A., Zhang, Z., Zimbra, D., Chen, H., & Nunamaker Jr, J. F. (2010). Detecting fake websites: The contribution of statistical learning theory. *Mis Quarterly*, 435-461.

Ajzen, I. (1985). From intentions to actions: A theory of planned behavior. In *Action control: From cognition to behavior* (pp. 11-39). Berlin, Heidelberg: Springer Berlin Heidelberg.

Ajzen, I. (1991). The theory of planned behavior. *Organizational behavior and human decision processes*, *50*(2), 179-211.

Alhawi, O. M., Baldwin, J., & Dehghantanha, A. (2018). Leveraging machine learning techniques for windows ransomware network traffic detection. *Cyber threat intelligence*, 93-106.

Alkhuzaie, A. S., & Asad, M. (2018). Operating cashflow, corporate governance, and sustainable dividend payout. *International Journal of Entrepreneurship*, *22*(4), 1-9.

Allam, Z., Asad, M., Ali, A., & Ali, N. (2021, December). Visualization of knowledge aspects on workplace spirituality through bibliometric analysis. In *2021 International conference on decision aid sciences and application (DASA)* (pp. 446-450). IEEE.

Allam, Z., Asad, M., Ali, N., & Malik, A. (2022, March). Bibliometric analysis of research visualizations of knowledge aspects on burnout among teachers from 2012 to January 2022. In *2022 International conference on decision aid sciences and applications (DASA)* (pp. 126-131). IEEE.

Ahmad Almansour, A. A. Z., Asad, M., & Shahzad, I. (2016). Analysis Of Corporate Governance Compliance And Its Impact Over Return On Assets Of Listed Companies In Malaysia. *Science International*, *28*(3).

Amir, A., & Asad, M. (2017). Consumer's Purchase Intentions towards automobiles in Pakistan. *Open Journal of Business and Management*, *6*(1), 202-213.

Asad, M., Aledeinat, M., Majali, T. E., Almajali, D. A., & Shrafat, F. D. (2024). Mediating role of green innovation and moderating role of resource acquisition with firm age between green entrepreneurial orientation and performance of entrepreneurial firms. *Cogent Business & Management*, *11*(1), 2291850.

Asad, M., Altaf, N., & Israr, A. (2020, October). Data analytics and SME performance: A bibliometric analysis. In *2020 International conference on data analytics for business and industry: Way towards a sustainable economy (ICDABI)* (pp. 1-5). IEEE.

Asad, M., Asif, M. U., Sulaiman, M. A. B. A., Satar, M. S., & Alarifi, G. (2023). Open innovation: the missing nexus between entrepreneurial orientation, total quality management, and performance of SMEs. *Journal of Innovation and Entrepreneurship*, *12*(1), 79.

Asad, M., Chethiyar, S. D. M., & Ali, A. (2020). Total quality management, entrepreneurial orientation, and market orientation: Moderating effect of environment on performance of SMEs. *Paradigms*, *14*(1), 102-108.

Asad, M., Haider, S. H., & Fatima, M. (2018). Corporate social responsibility, business ethics, and labor laws: A qualitative study on SMEs in Sialkot. *J. Legal Ethical & Regul. Isses*, *21*, 1.

Asad, M., Kashif, M., Sheikh, U. A., Asif, M. U., George, S., & Khan, G. U. H. (2022). Synergetic effect of safety culture and safety climate on safety performance in SMEs: does transformation leadership have a moderating role?. *International journal of occupational safety and ergonomics*, *28*(3), 1858-1864.

Asad, M., Majali, T. E., Aledeinat, M., Abdelkarim Almajali, D., & Akhorshaideh, A. H. O. (2023). Green entrepreneurial orientation for enhancing SMEs financial and environmental performance: Synergetic moderation of green technology dynamism and knowledge transfer and integration. *Cogent Business & Management*, *10*(3), 2278842.

Asad, M., Muhammad, R., Rasheed, N., Chethiyar, S. D., & Ali, A. (2020). Unveiling antecedents of organizational politics: An exploratory study on science and technology universities of Pakistan. *International Journal of Advanced Science and Technology*, *29*(6s), 2057-2066.

Asif, M. U., Asad, M., Bhutta, N. A., & Khan, S. N. (2021, November). Leadership behavior and sustainable leadership among higher education institutions of Pakistan. In *2021 Sustainable Leadership and Academic Excellence International Conference (SLAE)* (pp. 1-6). IEEE.

Asif, M. U., Asad, M., Kashif, M., & ul Haq, M. A. (2021, November). Knowledge exploitation and knowledge exploration for sustainable performance of SMEs. In *2021 Third International Sustainability and Resilience Conference: Climate Change* (pp. 29-34). IEEE.

Avtest, T. I. S. (2020). *Security Report* 2019/2020.

Bashir, A., & Asad, M. (2018). Moderating effect of leverage on the relationship between board size, board meetings and performance: A study on textile sector of Pakistan. *American Scientific Research Journal for Engineering, Technology, and Sciences (ASRJETS)*, *39*(1), 19-29.

Bilal, Z. O., & Sulaiman, M. A. (2021). Factors persuading customers to adopt Islamic banks and windows of commercial banks services in Sultanate of Oman. *Review of International Geographical Education Online*, *11*(4), 651-660.

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS quarterly*, *39*(4), 837-864.

Chethiyar, S. D. M., Asad, M., Kamaluddin, M. R. U., Ali, A., & Sulaiman, M. A. B. A. (2019). Impact of information and communication overload syndrome on the performance of students. *Opción: Revista de Ciencias Humanas y Sociales*, (24), 390-405.

Chethiyar, S. D. M., Asad, M., Kamaluddin, M. R. U., Ali, A., & Sulaiman, M. A. B. A. (2019). Impact of information and communication overload syndrome on the performance of students. *Opción: Revista de Ciencias Humanas y Sociales*, (24), 390-405.

Damer, N., Al-Znaimat, A. H., Asad, M., & Almansou, Z. A. (2021). Analysis of motivational factors that influence usage of computer assisted audit techniques (CAATS) by external auditors in Jordan. *Academy of Strategic Management Journal*, *20*, 1-13.

Damer, N., Al-Znaimat, A. H., Asad, M., & Almansou, Z. A. (2021). Analysis of motivational factors that influence usage of computer assisted audit techniques (CAATS) by external

auditors in Jordan. *Academy of Strategic Management Journal*, *20*, 1-13.

European Union Agency for Law Enforcement Cooperation. (EUROPOL) (2020). Pandemic Profiteering: How Criminals Exploit the COVID-19 Crisis. The Hague, The Netherlands: European Union Agency for Law Enforcement Cooperation. *https://www.europol.europa.eu/publications-documents/pandemic-profiteeringhowcriminals-exploit-covid-19-crisis.*

Al Fadhel, H., Aljalahma, A., Almuhanadi, M., Asad, M., & Sheikh, U. (2022). Management of higher education institutions in the GCC countries during the emergence of COVID-19: A review of opportunities, challenges, and a way forward. *The International Journal of Learning in Higher Education*, *29*(1), 83.

profitability measures on free cash flow; evidence from Pakistan stock exchange . *International Journal of Scientific & Technology Research*, 9(2), 3882-3889.

Majali, T. E., Alkaraki, M., Asad, M., Aladwan, N., & Aledeinat, M. (2022). Green transformational leadership, green entrepreneurial orientation and performance of SMEs: The mediating role of green product innovation. *Journal of Open Innovation: Technology, Market, and Complexity*, *8*(4), 191.

Malaysian National Cyber Security Agency. (2020). MyCERT – The Malaysian Computer Emergency Response Team. *https://www.cybersecurity.my/en/our_services/mycert/main/detail/2328/index.html.*

Monteith, S., Bauer, M., Alda, M., Geddes, J., Whybrow, P. C., & Glenn, T. (2021). Increasing cybercrime since the pandemic: Concerns for psychiatry. *Current psychiatry reports*, *23*, 1-9.

Norton Cybercrime Report. (2010). Norton's Cybercrime Report: The Human Impact Reveals Global Cybercrime Epidemic and Our Hidden Hypocrisy. *https://community.norton.com/en/blogs/symantec-cyber-education/norton%E2%80%99s-cybercrime-report-human-impact-reveals-global-cybercrime.*

Page, K., & Uncles, M. (2004). Consumer knowledge of the World Wide Web: Conceptualization and measurement. *Psychology & Marketing*, *21*(8), 573-591.

Pallant, J. (2020). *SPSS survival manual: A step by step guide to data analysis using IBM SPSS*. Routledge.

Potosky, D. (2007). The Internet knowledge (iKnow) measure. *Computers in Human behavior*, *23*(6), 2760-2777.

Qalati, S. A., Ostic, D., Sulaiman, M. A. B. A., Gopang, A. A., & Khan, A. (2022). Social media and SMEs' performance in developing countries: Effects of technological-organizational-environmental factors on the adoption of social media. *Sage Open*, *12*(2), 21582440221094594.

Qalati, S. A., Qureshi, N. A., Ostic, D., & Sulaiman, M. A. B. A. (2022). An extension of the theory of planned behavior to understand factors influencing Pakistani households' energy-saving intentions and behavior: a mediated–moderated model. *Energy Efficiency*, *15*(6), 40.

Zahid, H., Ali, S., Danish, M., & Sulaiman, M. A. B. A. (2022). Factors affecting consumers intentions to purchase dairy products in Pakistan: A cognitive affective-attitude approach. *Journal of International Food & Agribusiness Marketing*, 1-26.

Marican, S. (2005). *Kaedah penyelidikan sains sosial*. Prentice Hall/Pearson Malaysia.

Shahid Satar, M., Alarifi, G., Alkhoraif, A. A., & Asad, M. (2023). Influence of perceptual and demographic factors on the likelihood of becoming social entrepreneurs in Saudi Arabia, Bahrain, and United Arab Emirates–an empirical analysis. *Cogent Business & Management*, *10*(3), 2253577.

Sfakianakis, A., Douligeris, C., Marinos, L., Louren¸co, M., andRaghimi, O. (2019). *Enisa threat landscape report 2018: 15 top cyberthreats and trends*.

Singh, M. M., Frank, R., & Zainon, W. M. N. W. (2021). Cyber-criminology defense in pervasive environment: A study of cybercrimes in Malaysia. *Bulletin of Electrical Engineering and Informatics*, *10*(3), 1658-1668.

Sulaiman, M. A. B. A., & Asad, M. (2023). Organizational learning, innovation, organizational structure and performance evidence from Oman. In *ISPIM Conference Proceedings* (pp. 1-17). The International Society for Professional Innovation Management (ISPIM).

Sulaiman, M. A. B. A., Asad, M., Ismail, M. Y., & Shabbir, M. S. (2023). Catalyst role of university green entrepreneurial support promoting green entrepreneurial inclinations among youth: Empirical evidence from Oman. *International Journal of Professional Business Review: Int. J. Prof. Bus. Rev.*, *8*(8), 24.

Sulaiman, M. A. B. A., Asad, M., Shabbir, M. S., & Ismail, M. Y. (2023). Support factors and green entrepreneurial inclinations for sustainable competencies: Empirical evidence from Oman. *International Journal of Professional Business Review: Int. J. Prof. Bus. Rev.*, *8*(8), 25.

Ta'Amnha, M. A., Magableh, I. K., Asad, M., & Al-Qudah, S. (2023). Open innovation: The missing link between synergetic effect of entrepreneurial orientation and knowledge management over product innovation performance. *Journal of Open Innovation: Technology, Market, and Complexity*, *9*(4), 100147.

Tharshini, N. K., Hassan, Z., & Mas'ud, F. H. (2021). Cybercrime Threat Landscape amid the Movement Control Order in Malaysia. *International Journal of Business and Society*, *22*(3), 1589-1601.

TheStar. (2021). Retrieved from RM67.6mil lost due to cybercrimes early this year: *https://www.thestar.com.my/news/nation/2019/04/24/rm676mil-lost-due-to-cybercrimes.*

Tibi, M. H., Hadeje, K., & Watted, B. (2019). Cybercrime awareness among students at a teacher training college. *International Journal of Computer Trends and Technology*, *67*(6), 11-17.

Ullah, Z., Álvarez-Otero, S., Sulaiman, M. A. B. A., Sial, M. S., Ahmad, N., Scholz, M., & Omhand, K. (2021). Achieving organizational social sustainability through electronic performance appraisal systems: The moderating influence of transformational leadership. *Sustainability*, *13*(10), 5611.

Ullah, Z., Sulaiman, M. A. B. A., Ali, S. B., Ahmad, N., Scholz, M., & Han, H. (2021). The effect of work safety on organizational social sustainability improvement in the healthcare sector: The case of a public sector hospital in Pakistan. *International journal of environmental research and public health*, *18*(12), 6672.

Vedamanikam, M., & Chethiyar, S. D. M. (2023). Knowledge of Money Laundering and Rationalization of Money Mule Job Acceptance: A Study among Higher Education Students in Malaysia. *Pakistan Journal of Criminology*, *15*(3).

Vedamanikam, M., Chethiyar, S. D., & Awan, S. M. (2022). Job acceptance in money mule recruitment: Theoretical view on the rewards. *Pakistan Journal of Psychological Research*, *37*(1), 111-117.

Victor, S., ul Haq, M. A., Sankar, J. P., Akram, F., & Asad, M. (2021, December). Paradigm shift of promotional strategy from celebrity to social CEO. In *2021 International Conference on Decision Aid Sciences and Application (DASA)* (pp. 1016-1023). IEEE.

Vinet, L., & Zhedanov, A. (2011). A 'missing'family of classical orthogonal polynomials. *Journal of Physics A: Mathematical and Theoretical*, *44*(8), 085201.

Wei, L., & Zhang, M. (2008). The impact of Internet knowledge on college students' intention to continue to use the Internet. *Information Research: An International Electronic Journal*, *13*(3).

Xie, Z., Qalati, S. A., Limón, M. L. S., Sulaiman, M. A. B. A., & Qureshi, N. A. (2023). Understanding factors influencing healthcare workers' intention towards the COVID-19 vaccine. *PLoS One*, *18*(7), e0286794.

Yao, M. Z., & Linz, D. G. (2008). Predicting self-protections of online privacy. *CyberPsychology & Behavior*, *11*(5), 615-617.

Zafar, Z., Wenyuan, L., Bait Ali Sulaiman, M. A., Siddiqui, K. A., & Qalati, S. A. (2022). Social entrepreneurship orientation and enterprise fortune: An intermediary role of social performance. *Frontiers in Psychology*, *12*, 755080.